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

ЗАДАЧА ПРОЕКТА

Провести пилот Индекса кибермощи для:

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

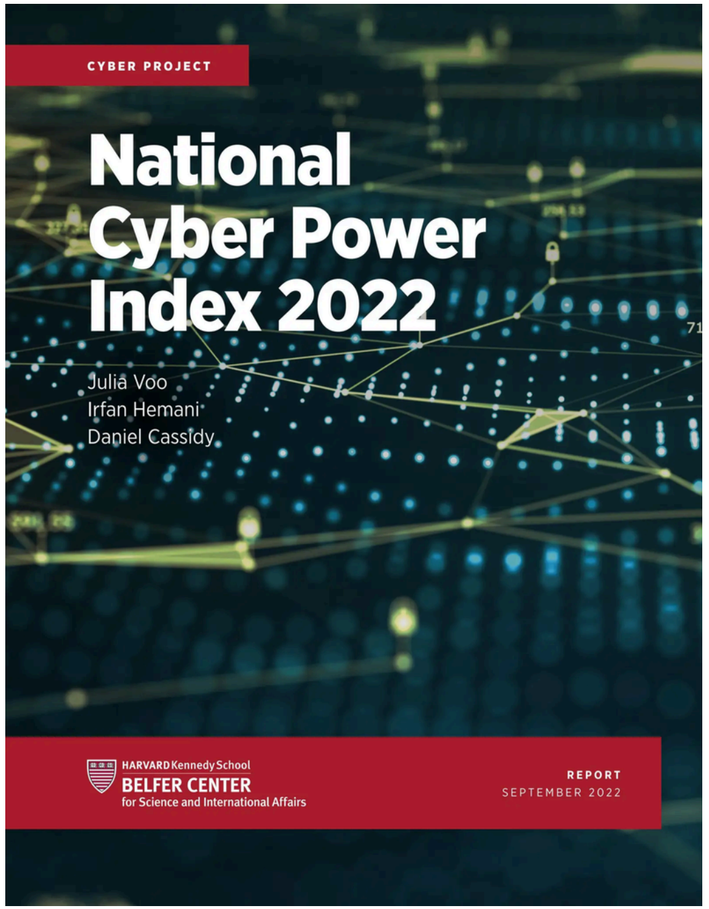
Работа над индексом

- **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.

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

ВЕБ-ПОРТАЛ

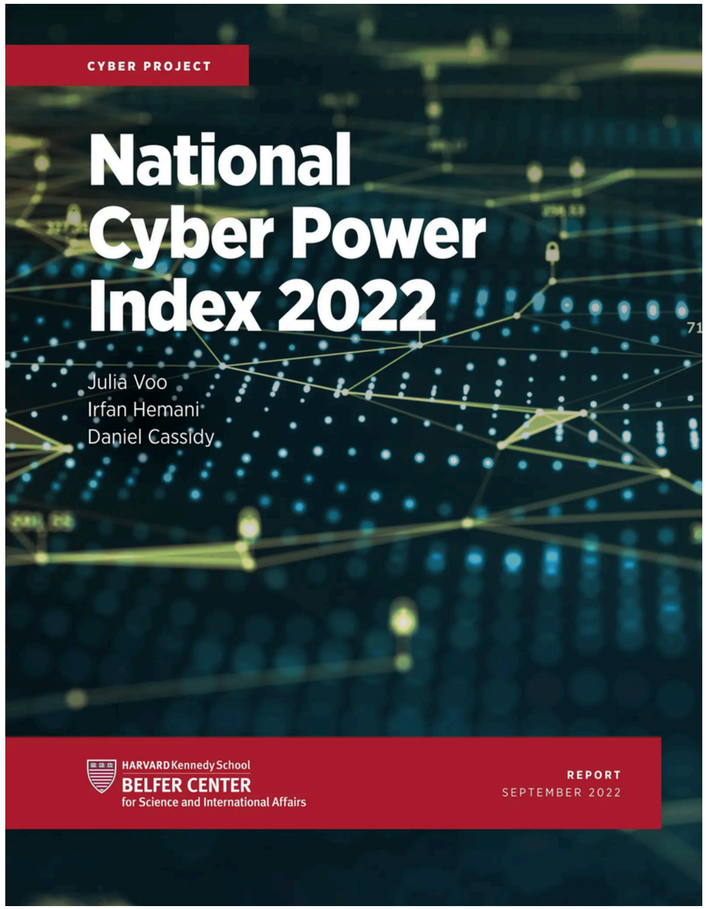
$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{8}\sum_{x=1}^{8} Capability_x \times Intent$$



СЛЕПЫЕ ЗОНЫ И МЕТОДОЛОГИЧЕСКИЕ УЯЗВИМОСТИ

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

- 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.



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.

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.

INTENT

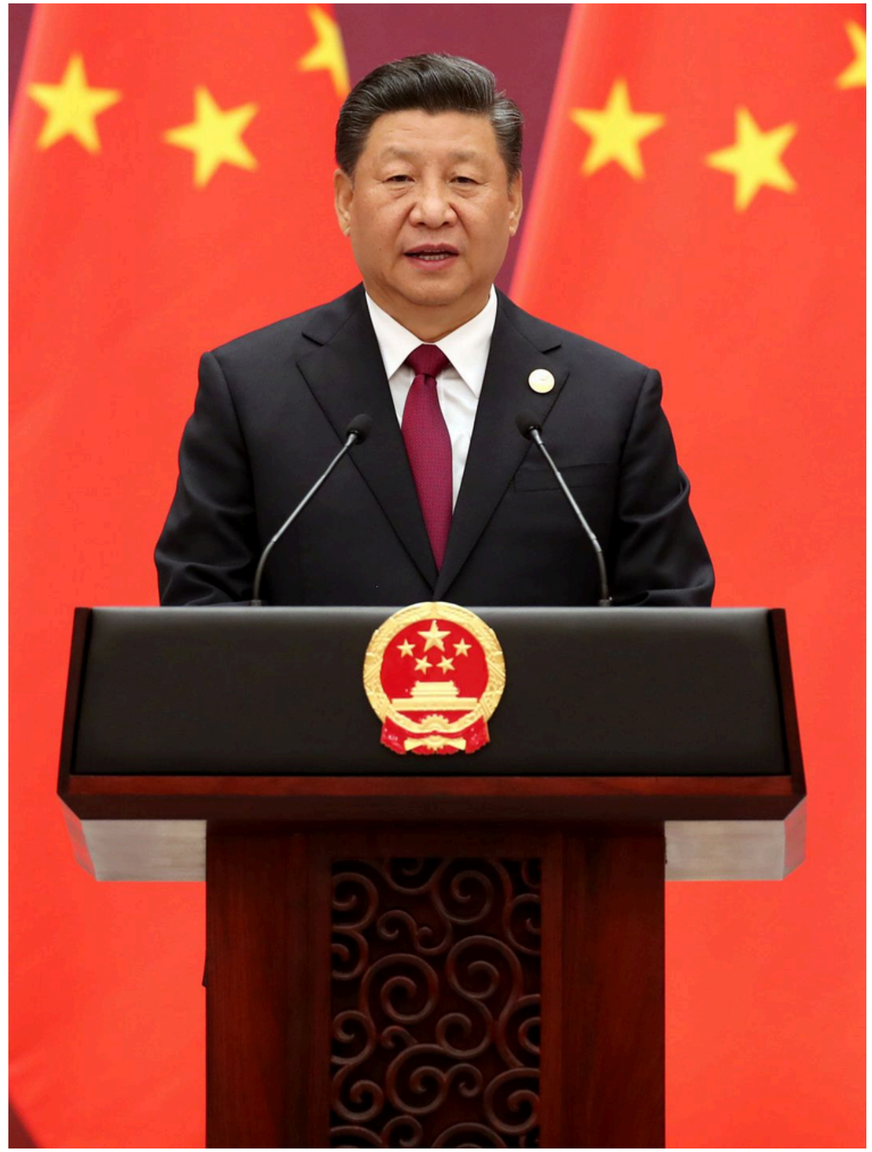
- Стратегические установки и цели, зафиксированные в нормативных документах, доктринах и официальных заявлениях.
- Отражает направленность и амбиции государства в области кибербезопасности и кибермощи.
- Показывает, что государство планирует или стремится делать, даже если фактические возможности пока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

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.

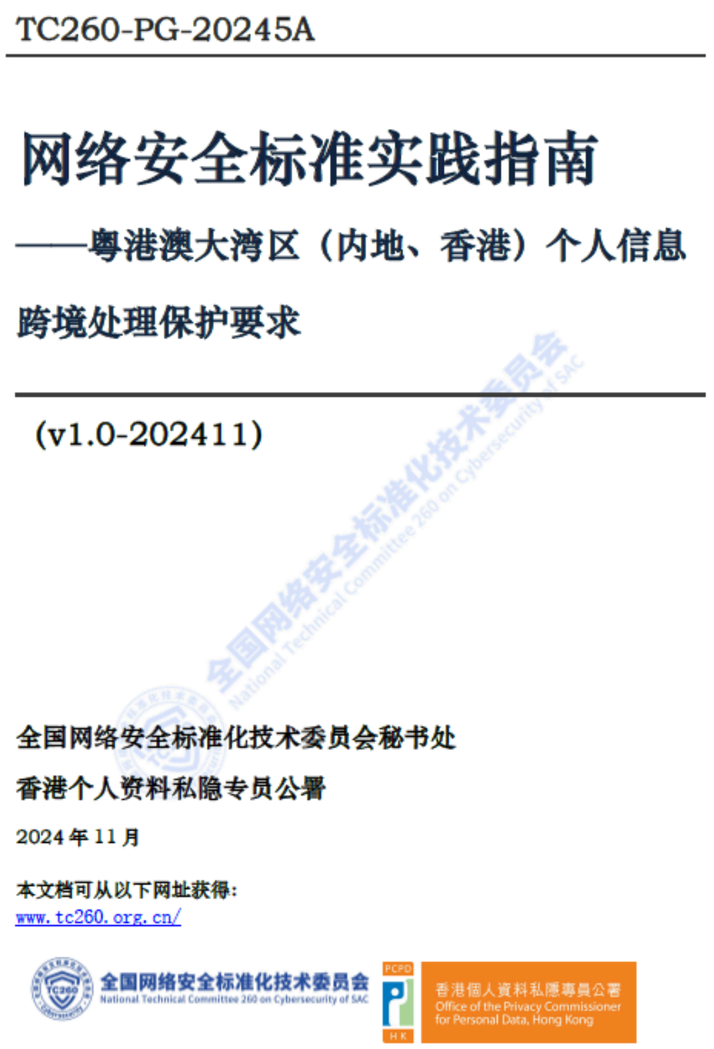
ПОЗИЦИОНИРОВАНИЕ КИТАЯ В ИНДЕКСЕ

- 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».



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

НУГ
CYBER SECURITY

@CYBERASIA25

ТЕЛЕГРАМ-
КАНАЛ

САЙТ


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •