black hat USA 2024

AUGUST 7-8, 2024

BRIEFINGS

A Framework For Evaluating National Cybersecurity Strategies

Fred Heiding, Alex O’Neill, Lachlan Price, Eric Rosenbach

Team

Fred Heiding

Research Fellow, Harvard
🐦 @_fredrikh01

Alex O'Neill

Independent Researcher

Lachlan Price

MPP Student and Research Assistant, Harvard

Eric Rosenbach

Lecturer in Public Policy, Harvard

Team

I HACKED THE KING OF SWEDEN

Fred Heiding

Research Fellow, Harvard
🐦 @_fredrikh01

Alex O'Neill

Independent Researcher

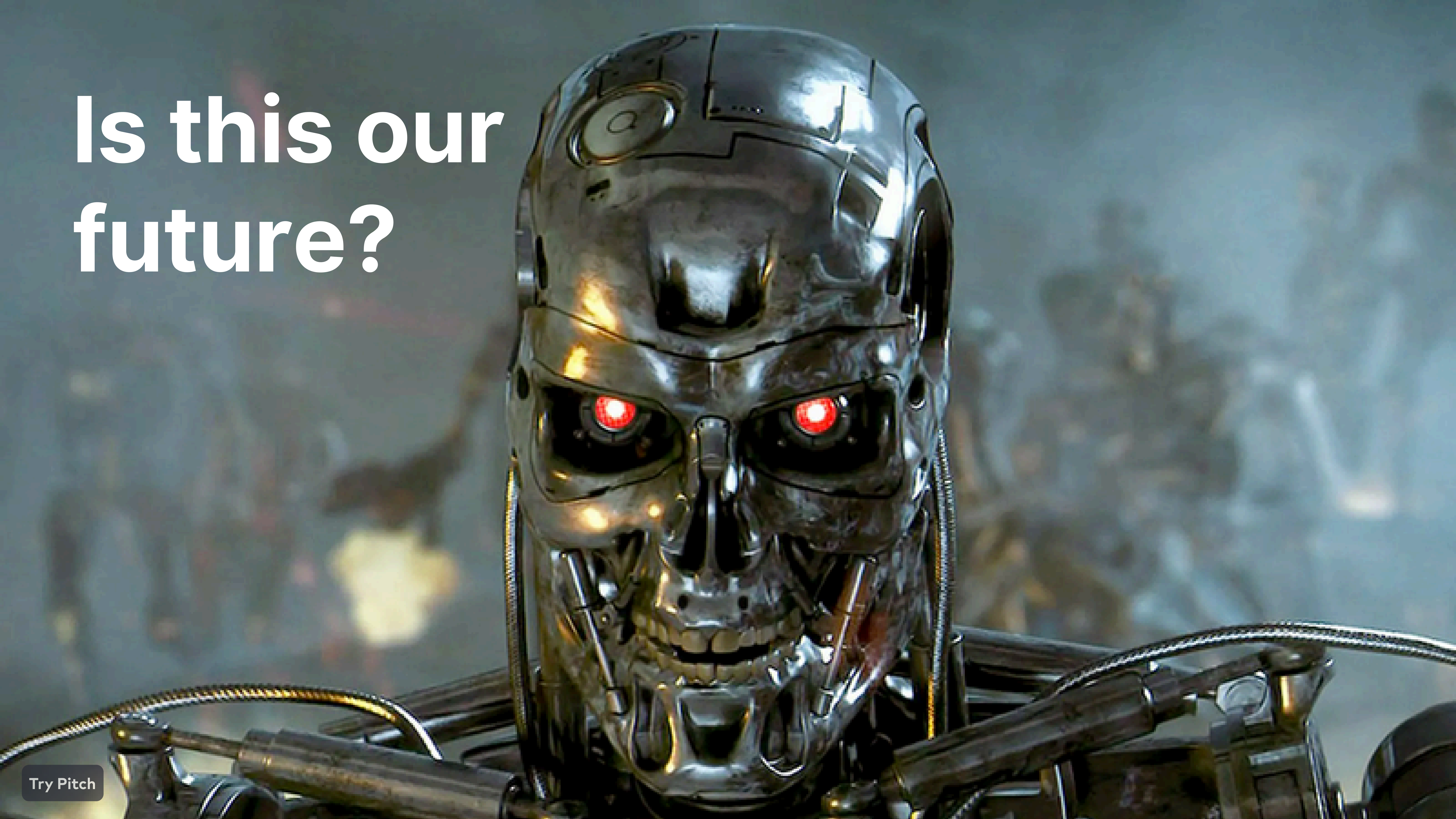
Lachlan Price

MPP Student and Research Assistant, Harvard

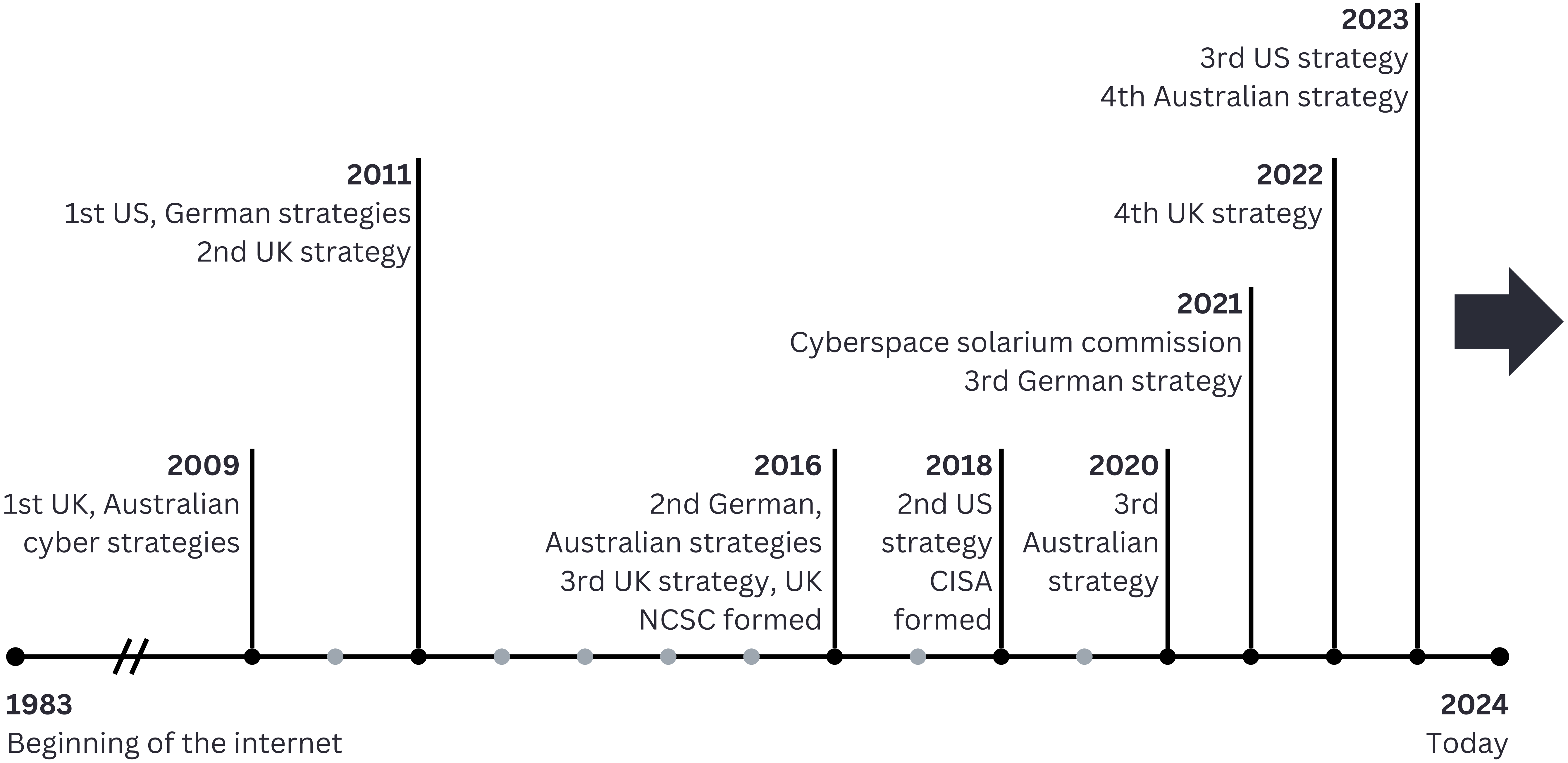
Eric Rosenbach

Lecturer in Public Policy, Harvard

Is this our future?



Cyber strategies are pretty new!



2009
1st UK, Australian cyber strategies

2011
1st US, German strategies
2nd UK strategy

2016
2nd German, Australian strategies
3rd UK strategy, UK NCSC formed

2018
2nd US strategy
CISA formed

2020
3rd Australian strategy

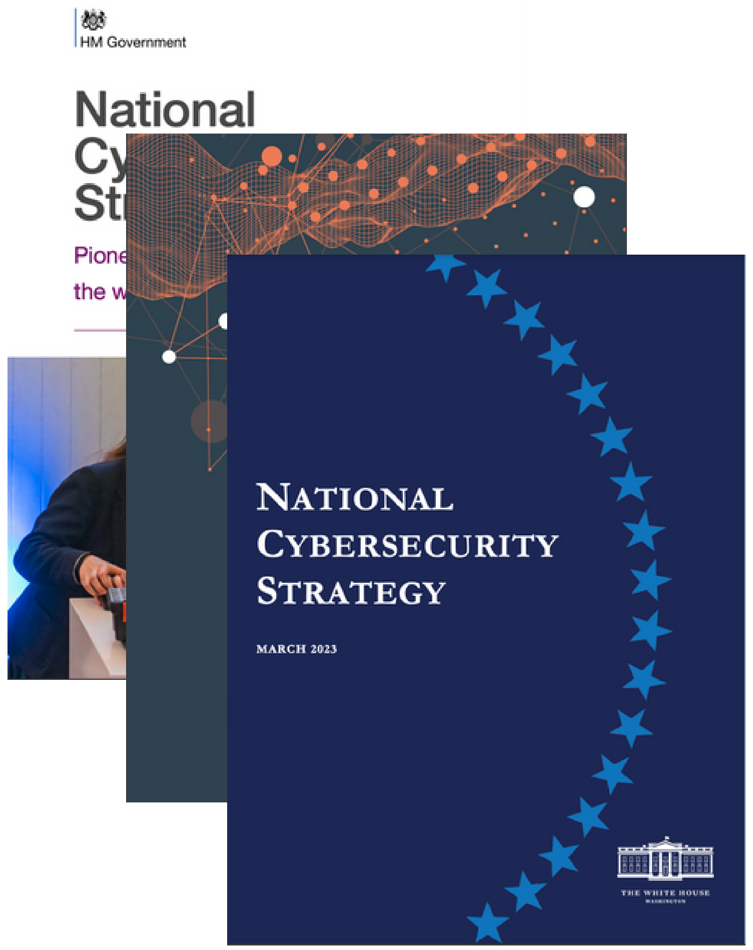
2021
Cyberspace solarium commission
3rd German strategy

2022
4th UK strategy

2023
3rd US strategy
4th Australian strategy

1983
Beginning of the internet

2024
Today



Do we know what we are doing?

Do we know what we are doing?

- What does a good cyber strategy entail?
- Who is the audience?
- Vision statement or practical policy guide?
- How technical should the strategy be?

How We Conducted Our Research

intro - **method (how)** - what we discovered - conclusion

Related work

- Other evaluation frameworks exist
    - NCSI, ITU, MIT
- Absolute vs relative scoring
- How to justify the scores?
- Can countries be scored in isolation?

Creating the Scorecard

Government selection

1. Strong cyber capabilities
2. Diversity (political, geographic, etc.)
3. Published after 2020
4. Publicly accessible + English

🇦🇺 🇦🇪 🇩🇪 🇮🇱 🇯🇵 🇸🇬 🇰🇷 🇬🇧 🇺🇸

Analysis

Evaluation Framework

- 268 criteria over 5 pillars

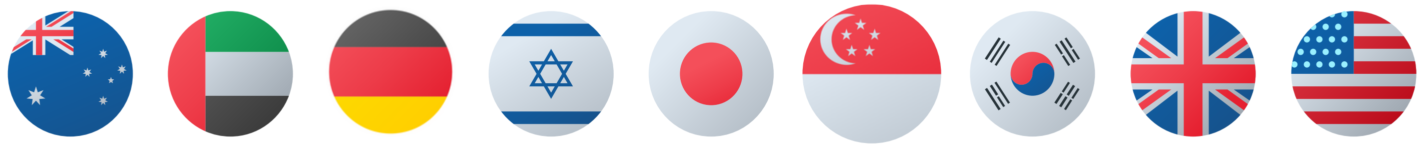
Interviews

- 25+ interviewees (9/23 - 7/24)
- Leading cyber experts and policymakers

Creating the Scorecard

Government selection

1. Strong cyber capabilities
2. Diversity (political, geographic, etc.)
3. Published after 2020
4. Publicly accessible + English



Analysis

Evaluation Fr

- 268 criteria

Interviews

- 25+ interviewees (9/23 - 7/24)
- Leading cyber experts and policymakers

🟩 Leading
🟨 Meeting the bar
🟥 Lagging

The Evaluation Framework

Codifying Responsibilities

- Government
- Private Sector
- Procedures
- *Who is responsible?*

Protecting People, Institutions, and Systems

- Critical Infrastructure
- Private entities
- Citizens
- Data
- Tech. regulations
- Forward defense

Generating Capacity and Capability

- Workforce development
- Skill development
- Market development

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

The Evaluation Framework

Codifying Responsibilities

- Government
- Private Sector
- Procedures
- Who is responsible for what?

Protecting People, Institutions, and Systems

- Government
- Critical Infra.
- Private orgs
- Citizens & data
- Forward defense

Generating Capacity and Capability

- Workforce development
- Skill development
- Market development

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

The Evaluation Framework

Codifying Responsibilities

- Government
- Private Sector
- Procedures
- Who is responsible for what?

Protecting People, Institutions, and Systems

- Critical Infrastructure
- Private entities
- Citizens
- Data
- Tech. regulations
- Forward defense

Generating Capacity and Capability

- Workforce
- Skills
- Market

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

The Evaluation Framework

Codifying Responsibilities

- Government
- Private Sector
- Procedures
- Who is responsible for what?

Protecting People, Institutions, and Systems

- Critical Infrastructure
- Private entities
- Citizens
- Data
- Tech. regulations
- Forward defense

Generating Capacity and Capability

- Workforce development
- Skill development
- Market development

Building Partnerships

- Intra-gov
- International
- Industry & Research

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

The Evaluation Framework

Codifying Responsibilities

- Government
- Private Sector
- Procedures
- Who is responsible for what?

Protecting People, Institutions, and Systems

- Critical Infrastructure
- Private entities
- Citizens
- Data
- Tech. regulations
- Forward defense

Generating Capacity and Capability

- Workforce development
- Skill development
- Market development

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

What We Discovered

intro - method (how) - **what we discovered** - conclusion

Strategy document summaries

	Date	Pages	Supporting documents
Australia	2023	64	Implementation plan, CI guidance
UAE	2023	31	Dubai cyber strategy
Germany	2021	133	CI strat., EU strat., Cyber. Compendium
Israel	2021	31	Data protection + IR framework
Japan	2021	68	CI cyber protection policy, Basic Act
Singapore	2021	35	Cybersecurity Act
South Korea	2024	24	US-ROK cyber cooperation framework
UK	2022	130	Gov’t cyber strategy, regulation review
USA	2023	39	Implementation plan, workforce strategy

The Cyber Scorecard

🟩 Leading 🟨 Meeting the bar 🟥 Lagging

	Codifying Responsib.	Protecting PI&S	Generating Capacity	Building Partnerships	Comm. Clear Policy
Australia	🟩	🟩	🟩	🟨	🟩
Germany	🟥	🟨	🟥	🟩	🟨
Japan	🟥	🟨	🟨	🟨	🟥
Singapore	🟩	🟩	🟩	🟩	🟨
South Korea	🟨	🟨	🟩	🟩	🟨
UK	🟩	🟩	🟩	🟨	🟨
USA	🟩	🟨	🟩	🟨	🟨

⋮

The Cyber Scorecard

🟩 Leading 🟨 Meeting the bar 🟥 Lagging

	Codifying Responsib.	Protecting PI&S	Generating Capacity	Building Partnerships	Comm. Clear Policy
Australia	🟩	🟩	🟩	🟨	🟩
Germany	🟥	🟨	🟥	🟩	🟨
Japan	🟥	🟨	🟨	🟨	🟥
Singapore	🟩	🟩	🟩	🟩	🟨
South Korea	🟨	🟨	🟩	🟩	🟨
UK	🟩	🟩	🟩	🟨	🟨
USA	🟩	🟨	🟩	🟨	🟨

⋮

The Cyber Scorecard

🟩 Leading 🟨 Meeting the bar 🟥 Lagging

	Codifying Responsib.	Protecting PI&S	Generating Capacity	Building Partnerships	Comm. Clear Policy
Australia	🟩	🟩	🟩	🟨	🟩
Germany	🟥	🟨	🟥	🟩	🟨
Japan	🟥	🟨	🟨	🟨	🟥
Singapore	🟩	🟩	🟩	🟩	🟨
South Korea	🟨	🟨	🟩	🟩	🟨
UK	🟩	🟩	🟩	🟨	🟨
USA	🟩	🟨	🟩	🟨	🟨

⋮

The Cyber Scorecard

🟩 Leading 🟨 Meeting the bar 🟥 Lagging

	Codifying Responsib.	Protecting PI&S	Generating Capacity	Building Partnerships	Comm. Clear Policy
Australia	🟩	🟩	🟩	🟨	🟩
Germany	🟥	🟨	🟥	🟩	🟨
Japan	🟥	🟨	🟨	🟨	🟥
Singapore	🟩	🟩	🟩	🟩	🟨
South Korea	🟨	🟨	🟩	🟩	🟨
UK	🟩	🟩	🟩	🟨	🟨
USA	🟩	🟨	🟩	🟨	🟨

⋮

The Cyber Scorecard

🟩 Leading 🟨 Meeting the bar 🟥 Lagging

	Codifying Responsib.	Protecting PI&S	Generating Capacity	Building Partnerships	Comm. Clear Policy
Australia	🟩	🟩	🟩	🟨	🟩
Germany	🟥	🟨	🟥	🟩	🟨
Japan	🟥	🟨	🟨	🟨	🟥
Singapore	🟩	🟩	🟩	🟩	🟨
South Korea	🟨	🟨	🟩	🟩	🟨
UK	🟩	🟩	🟩	🟨	🟨
USA	🟩	🟨	🟩	🟨	🟨

⋮

Strengths across most countries

- **Developing technical workforce and encouraging entrepreneurship**
- Prioritizing critical infrastructure cybersecurity
- Establishing partnerships with industry
- Addressing emerging threats like AI
- Using easy-to-understand language

Strengths across most countries

- Developing technical workforce and encouraging entrepreneurship
- **Prioritizing critical infrastructure cybersecurity**
- Establishing partnerships with industry
- Addressing emerging threats like AI
- Using easy-to-understand language

Strengths across most countries

- ✚ Developing technical workforce and encouraging entrepreneurship
- ✚ Prioritizing critical infrastructure cybersecurity
- ✚ **Establishing partnerships with industry**
- ✚ Addressing emerging threats like AI
- ✚ Using easy-to-understand language

Strengths across most countries

- ➕ Developing technical workforce and encouraging entrepreneurship
- ➕ Prioritizing critical infrastructure cybersecurity
- ➕ Establishing partnerships with industry
- ➕ **Addressing emerging threats like AI**
- ➕ Using easy-to-understand language

Strengths across most countries

- Developing technical workforce and encouraging entrepreneurship
- Prioritizing critical infrastructure cybersecurity
- Establishing partnerships with industry
- Addressing emerging threats like AI
- **Using easy-to-understand language**

Areas for improvement across most countries

- ⊖ **Protecting vulnerable populations**
- ⊖ Generating capability for non-technical cyber professionals
- ⊖ Building local and regional government capacity
- ⊖ Incentivizing private companies to prioritize cyber
- ⊖ Including specific timelines, measurable outcomes

Areas for improvement across most countries

- ⛔ Protecting vulnerable populations
- ⛔ **Generating capability for non-technical cyber professionals**
- ⛔ Building local and regional government capacity
- ⛔ Incentivizing private companies to prioritize cyber
- ⛔ Including specific timelines, measurable outcomes

Areas for improvement across most countries

- ⛔ Protecting vulnerable populations
- ⛔ Generating capability for non-technical cyber professionals
- ⛔ **Building local and regional government capacity**
- ⛔ Incentivizing private companies to prioritize cyber
- ⛔ Including specific timelines, measurable outcomes

Areas for improvement across most countries

- ⛔ Protecting vulnerable populations
- ⛔ Generating capability for non-technical cyber professionals
- ⛔ Building local and regional government capacity
- ⛔ **Incentivizing private companies to prioritize cyber**
- ⛔ Including specific timelines, measurable outcomes

Areas for improvement across most countries

- Protecting vulnerable populations
- Generating capability for non-technical cyber professionals
- Building local and regional government capacity
- Incentivizing private companies to prioritize cyber
- **Including specific timelines, measurable outcomes**

Questions arising from our work

- ? **How to balance regulation, incentives, and recommendations?**
- ? What roles and powers should a modern cyber security agency have?
- ? What are the best multilateral approaches to fighting cybercrime?
- ? What are the best models for national-regional/local cyber cooperation?

Questions arising from our work

- ? How to balance regulation, incentives, and recommendations?
- ? **What roles and powers should a modern cyber security agency have?**
- ? What are the best multilateral approaches to fighting cybercrime?
- ? What are the best models for national-regional/local cyber cooperation?

Questions arising from our work

- ? How to balance regulation, incentives, and recommendations?
- ? What roles and powers should a modern cyber security agency have?
- ? **What are the best multilateral approaches to fighting cybercrime?**
- ? What are the best models for national-regional/local cyber cooperation?

Questions arising from our work

- ? How to balance regulation, incentives, and recommendations?
- ? What roles and powers should a modern cyber security agency have?
- ? What are the best multilateral approaches to fighting cybercrime?
- ? **What are the best models for national-regional/local cyber cooperation?**

What We Discovered - Country Specific Highlights

intro - method (how) - **what we discovered** - conclusion

USA highlights

Strengths

- Shifting responsibility from users to private companies
- International cooperation and securing shared global resources
- Cyber Safety Review Board (CSRB)

Areas for improvement

- Fragmented data privacy laws
- Protecting vulnerable populations

USA highlights

Strengths

- Shifting responsibility from users to private companies
- International cooperation and securing shared global resources
- Cyber Safety Review Board (CSRB)

Areas for improvement

- Fragmented data privacy laws
- Protecting vulnerable populations

UK highlights

Strengths

- Govt-industry collaboration (Industry 100, Cyber Reserve,..)
- The Cyber Essentials model for organizational security

Areas for improvement

- Incentivizing critical infrastructure providers to improve protection
- Forward defense and disruption

UK highlights

Strengths

- Govt-industry collaboration (Industry 100, Cyber Reserve,..)
- The Cyber Essentials model for organizational security

Areas for improvement

- Incentivizing critical infrastructure providers to improve protection
- Forward defense and disruption

Australia highlights

Strengths

- Separation of assistance (incident response) vs. law enforcement
- Harmonization of CI regulations
- Protecting vulnerable groups (Cyber Wardens, commun. grants)

Areas for improvement

- Partnering with local and regional governments
- Civil society / non-profit sector
- Non-technical cyber professionals

Australia highlights

➕ Strengths

- Separation of assistance (incident response) vs. law enforcement
- Harmonization of CI regulations
- Protecting vulnerable groups (Cyber Wardens, commun. grants)
-

➖ Areas for improvement

- Partnering with local and regional governments
- Civil society / non-profit sector
- Non-technical cyber professionals

Singapore highlights

Strengths

- Securing government through Zero Trust
- Centralization of authority
- Regional leadership (ASEAN)

Areas for improvement

- Accountable parties and deadlines ("The government will...")
- Counter-ransomware strategy

Singapore highlights

Strengths

- Securing government through Zero Trust
- Centralization of authority
- Regional leadership (ASEAN)

Areas for improvement

- Accountable parties and deadlines ("The government will…")
- Counter-ransomware strategy

Highlights from other countries

➕ Strengths

- 🇩🇪 Intra-gvnmt. and regional partners.
- 🇩🇪 Gov. network modernization plan
- 🇯🇵 “Cybersec. for All”: vuln. pops. + SME
- 🇰🇷 Dismantling DPRK threat actors

➖ Areas for improvement

- 🇩🇪 Workforce development
- 🇩🇪 Forward defense
- 🇯🇵 Market development
- 🇰🇷 Protecting private organizations

Highlights from other countries

Strengths

- 🇩🇪 Intra-gvnmt. and regional partners.
- 🇩🇪 Gov. network modernization plan
- 🇯🇵 "Cybersec. for All": vuln. pops. + SME
- 🇰🇷 Dismantling DPRK threat actors

Areas for improvement

- 🇩🇪 Workforce development
- 🇩🇪 Forward defense
- 🇯🇵 Market development
- 🇰🇷 Protecting private organizations

Conclusion

intro - method (how) - what we discovered - **conclusion**

Next steps

Harvard Belfer Report: to be published in September/October

New scorecards: totalitarian states and smaller-budget states

New implementation area: evaluating national AI strategies

Reach out if you're interested: fheiding@seas.harvard.edu

Takeaways

There is no one-size-fits-all approach to national cyber strategy

Common shortcomings: protecting vulnerable populations & measurable goals

Every stakeholder contributes to national cyber security

- Government, industry, and individual
- How can your company contribute to national cybersecurity?
- How can you leverage cyber policy?

Takeaways

There is no one-size-fits-all approach to national cyber strategy

Common shortcomings: protecting vulnerable populations & measurable goals

Every stakeholder contributes to national cyber security

- Government, industry, and individual
- How can your company contribute to national cybersecurity?
- How can you leverage cyber policy?

Takeaways

There is no one-size-fits-all approach to national cyber strategy

Common shortcomings: protect vulnerable populations & measurable goals

Every stakeholder contributes to national cyber security

- **Government, industry, and individual**
- **How can your company contribute to national cybersecurity?**
- **How can you leverage cyber policy?**

The End

✉ Fred Heiding: fheiding@seas.harvard.edu

✉ Alex O'Neill: alex.oneill715@gmail.com

✉ Lachlan Price: lachlan_price@hks.harvard.edu