National Cybersecurity Strategies

Dr. Fred Heiding

Team

Fred Heiding

Postdoctoral researcher, Harvard

Alex O’Neill

Independent Researcher

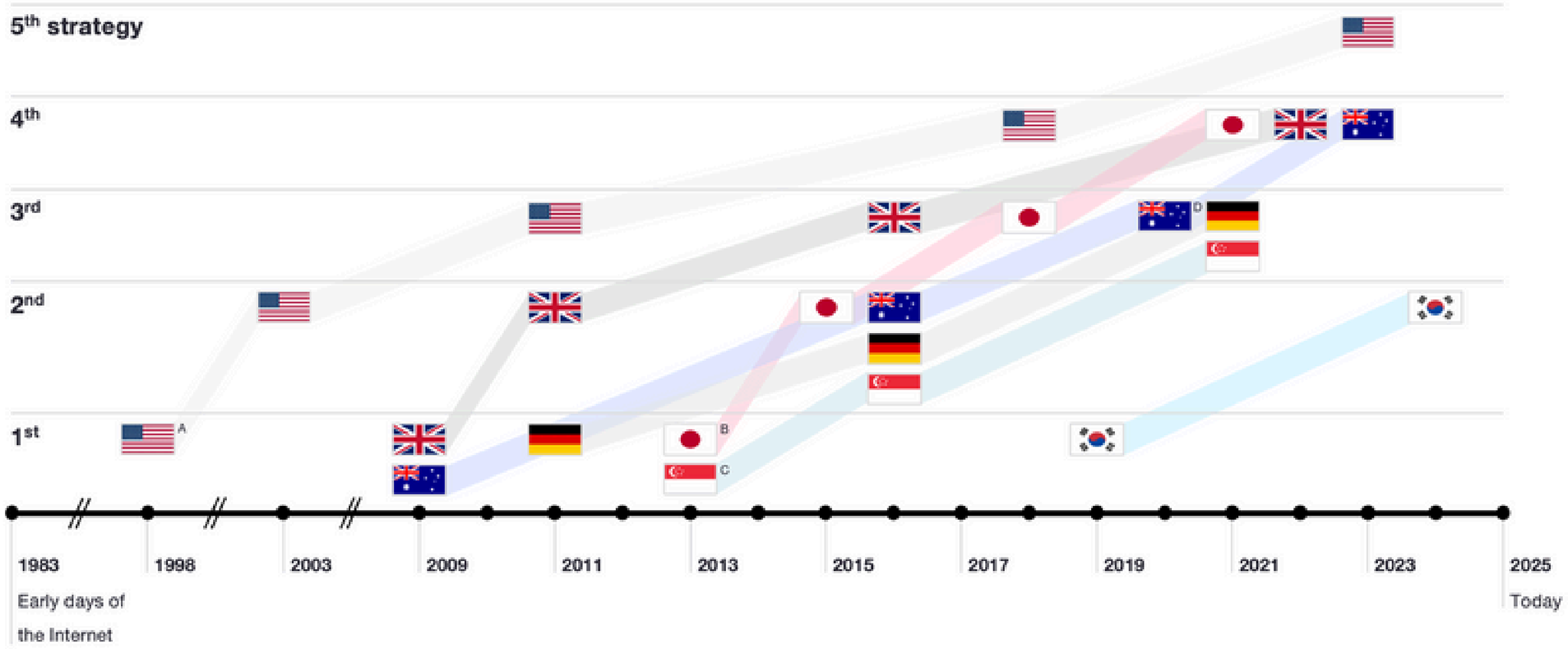
Lachlan Price

MPP Student and Research Assistant, Harvard

Eric Rosenbach

Lecturer in Public Policy, Harvard

National Cybersecurity Strategies



Notes: A. Refers to PDD 63, the first U.S. national cyber document; B. Ignores earlier acts and policy documents on information security strategy in 2000, 2006, 2009 and 2010; C. Ignores earlier 'Infocomm Security Masterplans' from 2005 and 2008; D. Ignores International Cyber Engagement Strategy documents in intervening years

Why do we do this?

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?

Evaluating Cyber Strategy

intro - **method** - results - conclusion

Evaluating Cyber Strategy

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

Evaluating Cyber Strategy

Analysis

Evaluation Framework

- 268 criteria over 5 pillars

Interviews

- 35 leading cyber experts

Relative difference

- Update scores based on other countries' performance

Initial country selection

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

Evaluating Cyber Strategy

Analysis

Evaluation Framework

- 268 criteria over 5 pillars

Interviews

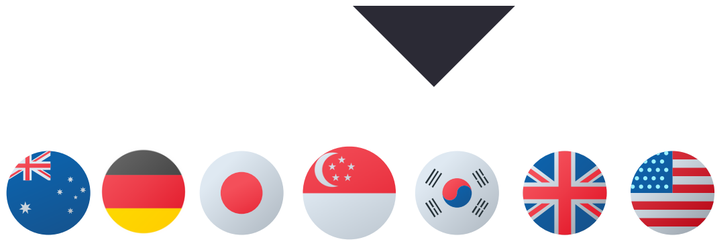
- 35 leading cyber experts

Relative difference

- Update scores based on other countries' performance

Initial count

1. Strong cyber ca
2. Diversity (political, geog
3. Published after 2020
4. Publicly accessible + English



Evaluation Framework

Protecting People, and Infrastructure

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

Generating Capacity

- Workforce
- Skills
- Market

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Codifying Responsibilities

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

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

Evaluation Framework

Protecting People, and Infrastructure

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

Generating Capacity

- Workforce
- Skills
- Market

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Codifying Responsibilities

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

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

Evaluation Framework

Protecting People, and Infrastructure

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

Generating Capacity

- Workforce
- Skills
- Market

Building Partnerships

- Intra-gov
- International
- Industry & Research

Codifying Responsibilities

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

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

Evaluation Framework

Protecting People, and Infrastructure

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

Generating Capacity

- Workforce
- Skills
- Market

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Codifying Responsibilities

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

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

Evaluation Framework

Protecting People, and Infrastructure

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

Generating Capacity

- Workforce
- Skills
- Market

Building Partnerships

- Domestic non-government
- Domestic government
- International cooperation

Codifying Responsibilities

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

Communicating Clear Policy

- Accessibility
- Comprehensiveness
- Accountability

Results

intro - method - **results** - conclusion

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
- 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**
- 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
- **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
- 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?**

Results -
Country Specific Highlights

intro - method - **results** - conclusion

USA highlights

Strengths

- Shifting responsibility from users to private companies
- International cooperation and securing shared global resources

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

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 threat actors (DPRK)

Areas for improvement

- Workforce development
- 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
- Market development
- Protecting private organizations

Conclusion

intro - method - results - **conclusion**

Takeaways

Common strengths

- Generating technical cyber competence
- Leveraging partnership

Common shortcomings

- Protecting vulnerable population groups and SMEs
- Private sector incentive alignment for cybersecurity
- Generating non-technical cyber competence

Takeaways

Common strengths

- Generating technical cyber competence
- Leveraging partnership

Common shortcomings

- Protecting vulnerable population groups and SMEs
- Private sector incentive alignment for cybersecurity
- Generating non-technical cyber competence

Takeaways

Harvard Belfer Report: *https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard*

Future work:

- Evaluating national security risks of AI model infrastructure
- Evaluating national security risks of phishing and online fraud

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

The End

Fred Heiding fheiding@hks.harvard.edu @fredheiding