Making Sense of Cyber Capabilities for Small States

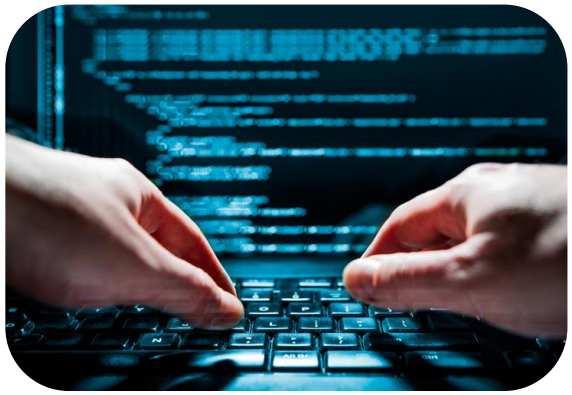
Stratbase ADR Institute
25 October 2022

Francis C. Domingo
Department of International Studies
De La Salle University

Scope of Lecture

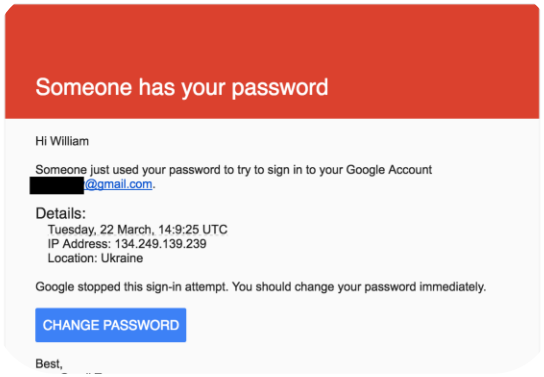
1. Context
2. Puzzle and argument
3. Theory and method
3. Analysis
4. Implications

Context: Cyber Operations

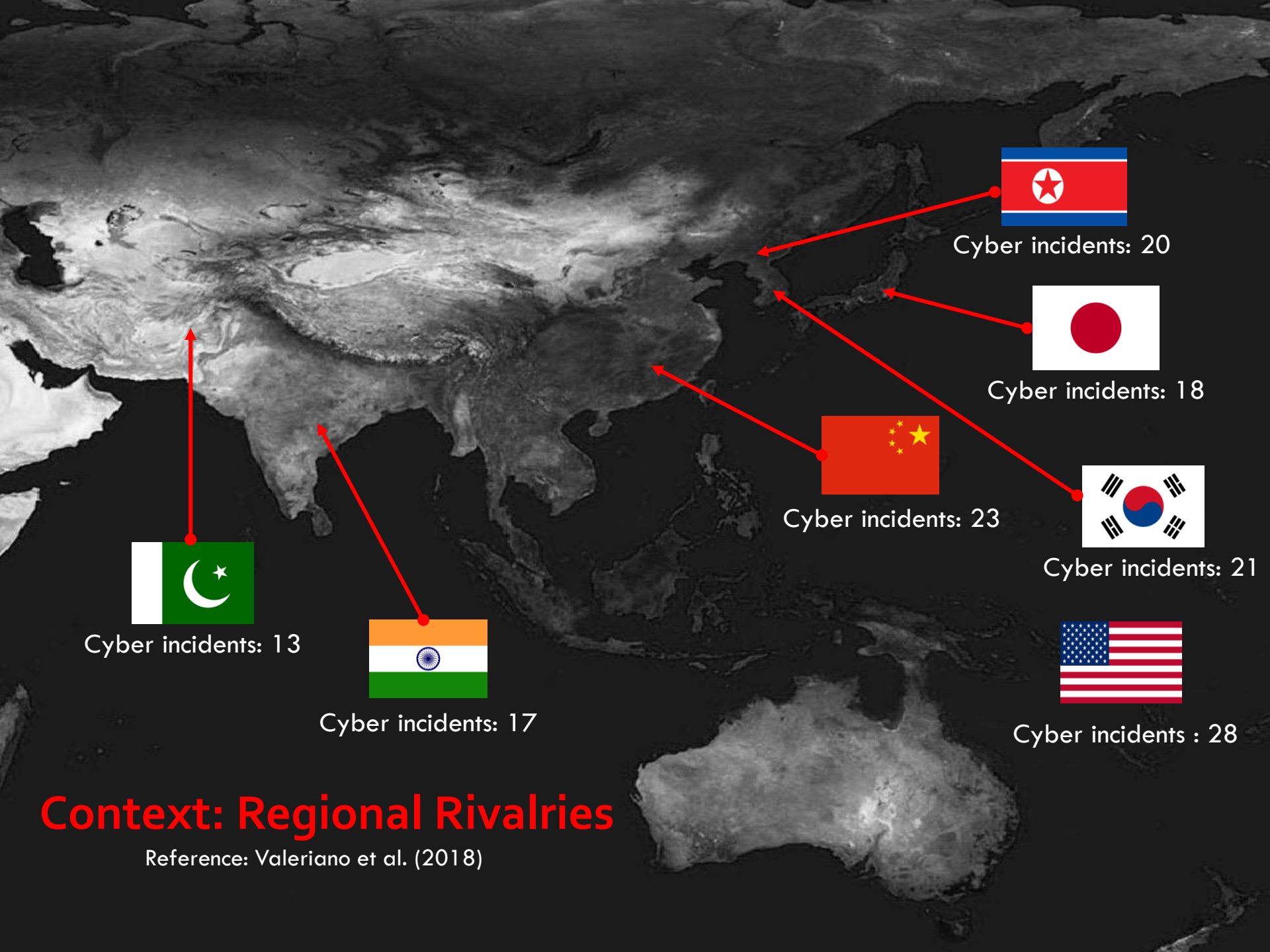


Espionage
(Gartzke et al., 2012; Harkett et al, 2022)

Sabotage
Rid, 2013; Rovner 2022



Subversion
(Buchanan, 2020; Maschmeyer, 2021)



Context: Regional Rivalries

Reference: Valeriano et al. (2018)

Context: Actors

Sponsor	Method	Motivation
State	vandalism, DDoS, intrusion, infiltration	intelligence collection, disruption or destruction of critical infrastructure
Criminals	crime	monetary gain
Activists	vandalism, DDoS	political protests to challenge the status quo
Hackers	vandalism, DDoS	bragging rights in the hacker community; thrill of challenge
Disgruntled insiders	intrusion, infiltration	damage and disrupt an organization
***Terrorists**	intrusion, infiltration	destroy, disable, or exploit critical infrastructures

Reference: Reveron, et al. (2012); Valeriano et al. (2015)

Puzzle and Argument

Why do small states develop cyber capabilities despite its obscure strategic value?

Neoclassical Realism

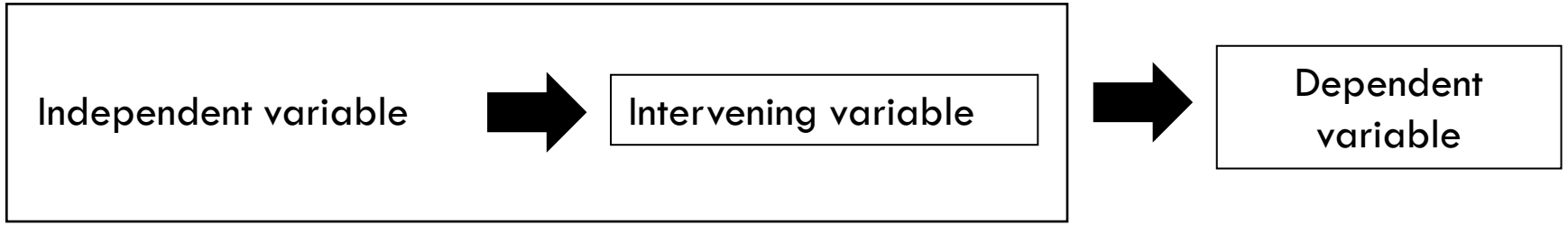
Systemic Level
Distribution of power

+

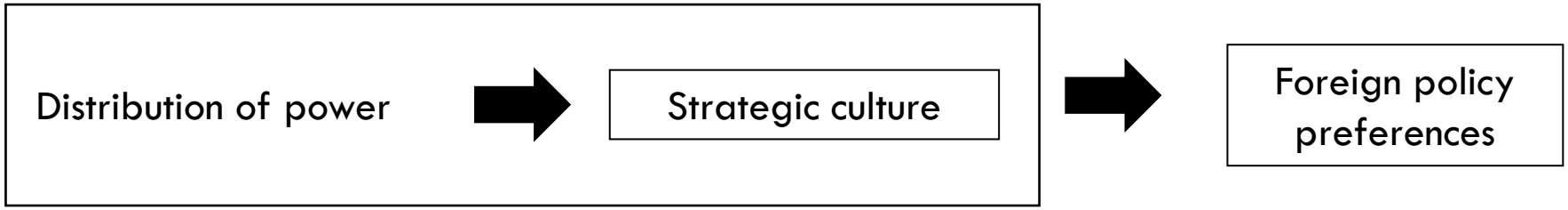
State Level
Technology-oriented" strategic culture

Theory: Neoclassical Realism

Variables of Neoclassical Realism



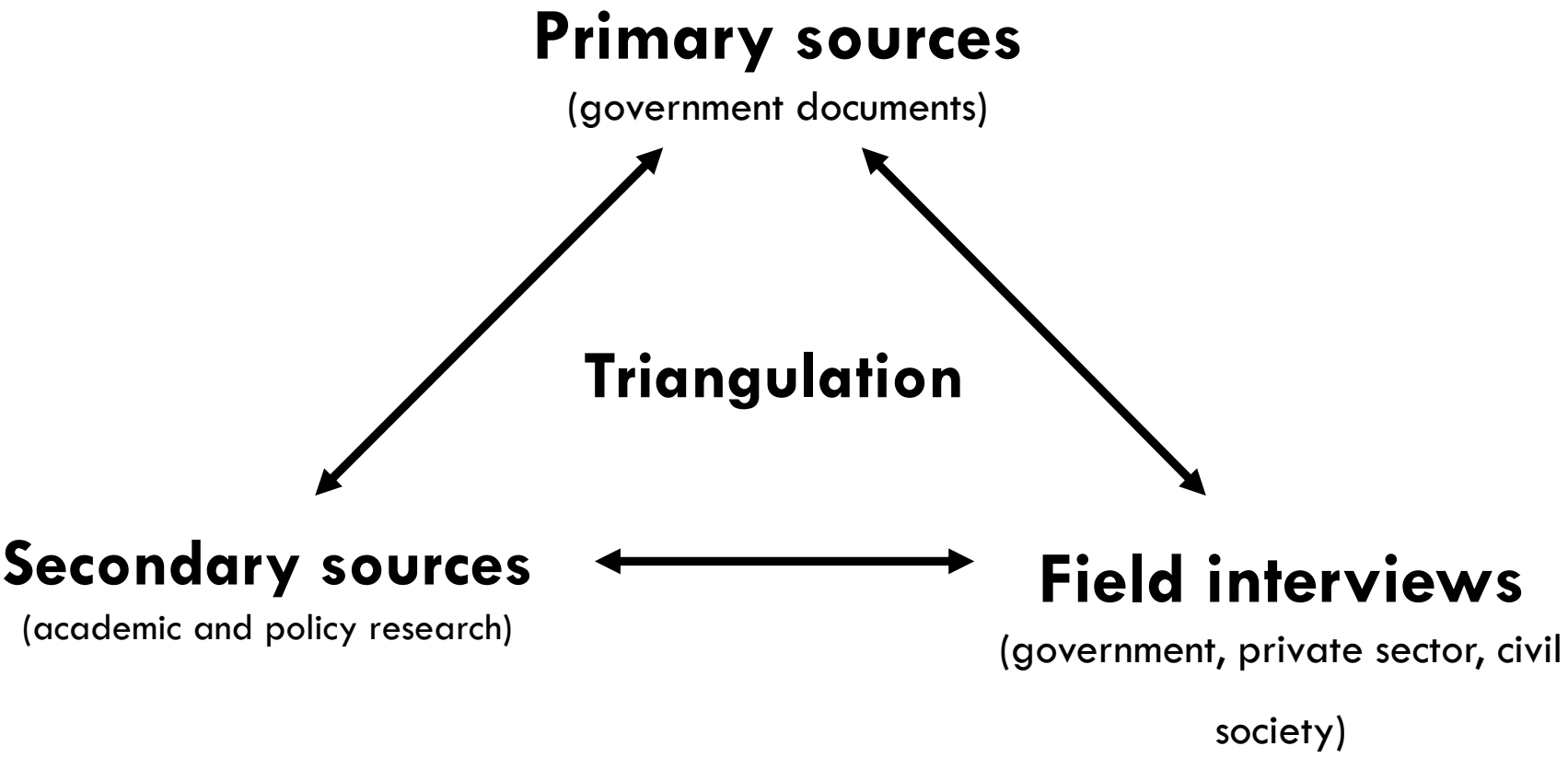
Conceptual framework



Applied framework

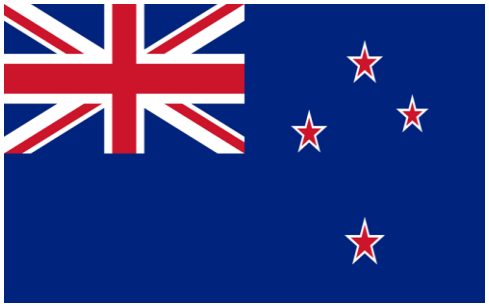
Reference: Domingo (2022)

Data Collection



Data Analysis: Comparative Method

- ✓ "Smallness" (population, foreign policy, military)
- ✓ Network readiness (use of technology)
- ✓ Cyber capabilities (evidence of cyber operations)
- ✓ Geographic location (Asia-Pacific Region)



Reference: Domingo (2022)

Data Analysis I: Theory Testing

Variables	Themes	Qualitative Indicators
Distribution of power	**Great power rivalry**	• Great powers that have interests in the region • Evidence of cyber conflict
	Military expenditures	• Increase in military spending • Evidence of expenditures for cyber capabilities
	Arms transfers	• Increase in the transfer military weapons • Evidence of cyber capabilities
Strategic culture	**Network readiness**	• Measurement of environment, readiness, usage, and impact of ICT by the WEF
	Relevance of technology for military affairs	• Indications of a technology-driven modernisation • Evidence of military upgrades focused on cyber capabilities
	Relevance of cyber security	• Recognition of cyber threats as a national security issue • Existence of an official strategy for addressing cyber threats

Reference: Domingo (2022)

Data Analysis I: Theory Testing

Variables	Themes	Qualitative Assessment
Distribution of power	**Great power rivalry**	• Singapore (affected) • New Zealand (affected) • Brunei (affected)
	Military expenditures	• Singapore (high) • New Zealand (low) • Brunei (low)
	Arms transfers	• Singapore (high) • New Zealand (low) • Brunei (low)
Strategic culture	**Network readiness**	• Singapore (high) • New Zealand (moderate) • Brunei (low)
	Relevance of technology for military affairs	• Singapore (high) • New Zealand (moderate) • Brunei (low)
	Relevance of cyber security	• Singapore (high) • New Zealand (high) • Brunei (moderate)

Reference: Domingo (2022)

Data Analysis II: Assessing Cyber Capabilities

Extreme

Routine

Traditional	Network-enabled
Military action (war, deterrence, compellence)	**Military action** (cyber deterrence, cyber compellence)
Political Interventions (sabotage, subversion)	**Political Interventions** ("cyber sabotage", hacktivism)
Negative sanctions (boycotts, embargoes, laser sanctions, restrictions on cultural contacts)	**Negative sanctions** (no equivalent)
Positive sanctions (aid, trade agreements, public diplomacy)	**Positive sanctions** (no equivalent)
Diplomacy (discussions/negotiations)	**Diplomacy** (digital diplomacy)

Table 5: Traditional and networked-enabled foreign policy

Data Analysis II: Assessing Cyber Capabilities

	Diplomacy	Negative Sanctions	Positive Sanctions	Political Intervention	Military Action
Singapore	Useful	No equivalent	No equivalent	Useful	Useful
New Zealand	Useful	No equivalent	No equivalent	Not useful	Not useful
Brunei	Useful	No equivalent	No equivalent	Not useful	Not useful

Implications for the Region

1. **Normality of cyber conflict. L**ow-level cyber conflict is likely to be an enduring feature of state interactions in the region
2. **Cyber evolution.** Network technologies have an evolutionary (not revolutionary) impact on the strategy and foreign policies of small states in the region
3. **Public-private partnerships.** Importance of developing public private partnerships in addressing cyber security issues

Implications for the Philippines

1. **Strategy.** Building on the *National Cybersecurity Plan 2022* is crucial for strengthening the defense posture of the Philippines

2. **Diplomacy.** Cyber diplomacy is necessary tool for less powerful states with limited resources

3. **Capability.** Leveraging the Philippine-U.S. alliance in enhancing the capacity for cyber operations

References

Daddow, O. (2017). *International Relations Theory* 3rd ed. California, USA: Sage Publications.

Domingo, F. (2022). *Making Sense of Cyber Capabilities for Small States*. London: Routledge.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace *Security Studies*, 24(2), 316-348.

Gray, C. S. (2013). *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle, PA: U.S. Army War College Press.

Halperin and Heath (2020). *Political Research: Methods and Practical Skills* 3rd ed. Oxford: Oxford University Press.

Maschmeyer, L. (2021). The Subversive Trilemma Why Cyber Operations Fall Short of Expectations. *International Security*, 46(2), pp. 51–90.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35 (1), 5-32.

Schmitt, M. (eds.) (2017). *Tallinn Manual 2.0 on The International Law Applicable To Cyber Operations*. Cambridge: Cambridge University Press.

Valeriano, B., Jensen, B. & Maness, R. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Viotti, P. and Kaupi, M. (2012). *International Relations Theory 5th Ed*. London: Pearson Education, Inc.

Waltz, K .(2010). *Theory of International Politics* Illinios, U.S.: Waveland Press. (Original work published in 1979).

Whyte, C. and Mazanec, B. (2018). *Understanding Cyber Warfare: Politics, Policy and Strategy*. London: Routledge.

Thank you for your attention.

Contact

francis.domingo@dlsu.edu.ph

@frcdlive