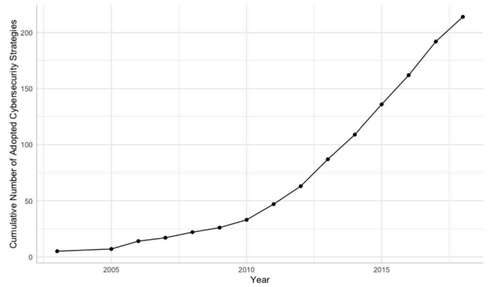
The United Nations Debates over Cybersovereignty:
The Global Diffusion of Cybersecurity Strategies

Nadiya Kostyuk

Department of Political Science, Gerald R. Ford School of Public Policy, University of Michigan, Ann Arbor

Puzzle

Figure 1: ADOPTION OF NATIONAL CYBERSECURITY STRATEGIES OVER TIME



Source: Author's calculations based on countries' data.

Research question: What drives the diffusion of cybersecurity strategies?
Answer: The adoption of such strategies by nations with similar preferences on cybersovereignty

Theory

Main Argument: The adoption of cybersecurity strategies—especially the first strategy—motivates governments to think about the role the Internet plays within their society, the challenges and opportunities it presents, and whether and how they want to regulate it. Before they make this important decision, I argue that nations observe the choices of other nations that share similar views on this subject.

Two views on cybersovereignty:

1. ***Anti-cybersovereignty***
   Leader: The United States
   Position: a single Internet
2. ***Pro-cybersovereignty***
   Leaders: Russia and China
   Position: state control over the Internet

Alternative Explanations:

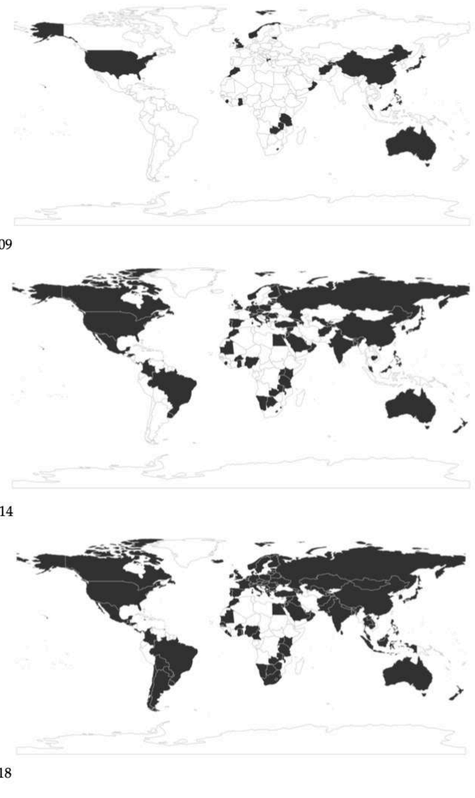
1. Cultural similarity
2. Expert communities
3. Harmonization after partners
4. Prestige
5. Regime type and similarity
6. Threat Environment

Hypothesis

If a country shares the same view on Internet governance with other nations that adopted national cybersecurity strategies in year $t-1$, then the country is likely to adopt its first national cybersecurity strategy in year t.

Data

Figure 2: DIFFUSION OF CYBERSECURITY STRATEGIES (2000-2018)



Source: National Cybersecurity Strategies Data (NCSS), collected by the author

- *Dependent Variable:* Adoption of the first cybersecurity strategy (Source: NCSS)
- *Main Predictor:* Cybersecurity strategies adopted by countries with similar preferences on cybersovereignty
  - *Cybersovereignty Preferences:* UNGA votes on resolutions on the topic of national sovereignty (Voeten, Strezhnev and Bailey 2017)

Method

Method: Cox-Proportional Hazard Model:

$$log(H(t; X_i([t-1]), y_i([t-1]))) \propto W_i([t-1])y_{-i}([t-1])\beta_1 + X_i([t-1])\beta_2,$$

- $log(H(t,X_i([t\text{-}1]), y_i([t\text{-}1])$: the log of a hazard ratio that stands for the relative risk of country *I* adopting a cybersecurity strategy at time *t;*
- $W_i([t\text{-}1])y_{-i}([t\text{-}1])$: a *n x n* spatial weights matrix that captures country *i*'s neighborhood in *t-1,* specifically

$$W_i([t-1]) * y_{-i}([t-1]) = \sum_{i=1,\ldots,N} W_{i,-i}([t-1]) * y_{-i}([t-1]).$$

Results

	Model 1 *Base*	Model 2 *Cultural Similarity*	Model 3 *Cultural Similarity*	Model 4 *Cultural Similarity*
Strategies Weighted by Cybersovereignty Partners	+	+	+	+
Strategies Weighted by Colonial Partners		**NE**		
Strategies Weighted by Linguistic Partners			**NE**	
Strategies Weighted by Neighbors				**NE**
Democracy and Internet Users (log)	+	+	+	+

	Model 5 *Expert Communities*	Model 6 *Harmonization after partners*	Model 7 *Harmonization after partners*	Model 8 *Harmonization after partners*
Strategies Weighted by Cybersovereignty Partners	+	+	+	+
Strategies Weighted by IGO Partners	**NE**			
Strategies Weighted by Allies		**NE**		
Strategies Weighted by Trading Partners			**NE**	
Strategies Weighted by UN Partners				**NE**
Democracy and Internet Users (log)	+	+	+	+

	Model 9 *Prestige*	Model 10 *Regime Similarity*	Model 11 *Threat Environment*
Strategies Weighted by Cybersovereignty Partners	+	+	+
IGO Membership	**NE**		
Strategies Weighted by Regime Partners		**NE**	
Threat Environment			**NE**
Democracy and Internet Users (log)	+	+	+

Note: **NE:** no effect; blank cell: variables were not included in the models

Discussion

Question: *what drives a state's decision to develop its defensive cybercapabilities in the form of strategies?*

Answer:

- NOT threat environment (Craig & Valeriano 2016)
- Diffusion of these capabilities occur along the blocks of nations with distinct preferences on cybersovereignty

This finding is robust to:

1. Alternative network measures
2. Cumulative influence of alternative network measures
3. Alternative measure of adopted strategies
4. Alternative model specification

Future Research

1. Vertical or temporal variation in strategy evolution (i.e., other stages of policy development)
2. Horizontal variation in strategy evolution (i.e., branching out different strategies to different governmental agencies)
3. Content analysis

References

1. Craig, Anthony and Brandon Valeriano. 2016. "Securing Cyberspace: The Drivers of National Cyber Security Policy." *Presented at the International Studies Association Conference.*
2. Voeten, Erik, Anton Strezhnev and Michael Bailey. 2017. "United Nations General Assembly Voting Data." **URL:** *http://hdl.handle.net/1902.1/12379*

Contact Information

Email: Nadiya@umich.edu
Website: http://www-personal.umich.edu/~nadiya/index.html