Rethinking Conditions for Authoritarian Regime Continuity in Asia in Relation to Cyberspace

Elif Sercen Nurcan

Meiji University Graduate School of Political Science and Economics

Ritsumeikan APU Presentation

November 15, 2020

Content

- Introduction

1. Cyberspace and the State
2. Research Question and Hypothesis
3. Four Generations of Controls in Cyberspace
4. Findings on Turkey, Thailand, China, and Singapore
5. Conclusions

Introduction

Introduction

- Theme: Utilization of cyberspace by authoritarian states
  - Different levels of economic development or different political systems but similar goals
- Research Question: What are the common characteristics of involvement in cyberspace by varying authoritarian regime types?
- Link to PhD research centered on the role of the state in cybersecurity in Japan

1. Cyberspace and the State

Cyberspace

- **Cyberspace** describes the widespread, "interdependent network of information technology infrastructure which includes the Internet, telecom networks, computer systems and embedded processors and controllers in various industries."
  - Became a buzzword in the 1990s as Internet, networking, and digital communication became widespread (Strate, 1999).

Strate, Lance (1999). "The varieties of cyberspace: Problems in definition and delimitation". Western Journal of Communication. 63 (3): 382–83. doi:10.1080/10570319909374648.
Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. 2015. *Democratic governance challenges of cyber security*. DCAF HORIZON 2015 WORKING PAPER No. 1.

Cyberspace and Politics

- Cyberspace as an area of national security, next to land, air, sea, and space
- An issue of national security as well as politics

Main Aspects of Cyberspace

- Three main aspects of cyberspace:

1. Defense: Security of military operations and critical public infrastructure
2. Economic: Protection of IPs, stock markets, and unhindered economic activities of private sector
3. Political: Continuation of political processes such as elections, maintenance of state legitimacy, regime continuity

- These aspects are often interlinked.

Table 1: Actor Classification in Cyberspace

Actor	Motivation		
	Self satisfaction /Personal belief	Economic benefit	Organized faith /National security
State			Public safety
Organization		Cyberintelligence	
Group	Hacktivists Hacker(s)	Cybercrime	Cyberterror
Individual	Hobbyist		

佳山こうせつ. 2015. Last accessed on May 14, 2020. *高度標的型攻撃対策に向けたシステム設計ガイド～感染することを前提とした「防御グランドデザイン」に向けたシステム設計の勘所～. https://www.ipa.go.jp/files/000045950.pdf.*

Sigholm, Johan. 2016. «Non-State Actors in Cyberspace Operations.» *Journal of Military Studies,* Volume 4, Issue 1. Last accessed on May 14, 2020. DOI: https://doi.org/10.1515/jms-2016-0184.

Renaissance of the State

- After Cold War, there was the expectation that globalization would bring an era of global governance.
  - "History" had ended (Francis Fukuyama, 1992, *The End of History and the Last Man*)
- By the end of 2010s, these expectations failed to materialize. The state, especially the authoritarian model, made a comeback.
  - Key examples include but are not limited to, Russia's growing separation from international bodies such as the G8 (2014), Brexit (2016), rise of isolationism in the US (since 2016), and the management of current COVID-19 outbreak crisis.

State and Cybersecurity

- Different utilization levels and purposes of interaction with cyberspace in each state
- Some focus on the political aspect.
  - Authoritarian states engage in cyberspace for regime survival and empowerment

2. Research Question and Hypothesis

Research Questions

- Theme: Utilization of cyberspace by authoritarian states
  - Different levels of economic development or different political systems but similar goals
- Research Question: What are the common characteristics of involvement in cyberspace by varying authoritarian regime types?

Hypothesis

- If certain characteristics of cyberspace utilization by the state can be observed within an authoritarian regime, then it is expected that cyberspace aids regime survival and empowerment.
- These characteristics are:

1. possession of first, second, third, and fourth-generation controls,
2. employment of national security rhetoric, and
3. lack of embeddedness in global governance system.

Structure and Methodology

- Two comparative analyses of four cases from Asia in pairs
- First pair of comparative analysis: Turkey and Thailand
  - To highlight the characteristic of employment of national security rhetoric
  - Similar military junta experiences with key differences
- Second comparative analysis: China and Singapore
  - To highlight the characteristic of lack of embeddedness in global governance
  - Similar high levels of economic connectivity with key differences in governance
- Deibert (2015) analysis on first, second, third, and fourth generations of cyberspace controls as toolkit of authoritarian regimes
  - Applied to four cases

Disclaimer

- Authoritarian states as well as democratic ones contain all three characteristics at differing levels. However, the goals and results are not the same.
- No deep debate on concept definitions (what is democracy, how is a state determined to be authoritarian etc.)
  - Turkey as a dominant party authoritarian regime since 2002
  - Thailand as a military authoritarian regime
  - Singapore as a regime without any peaceful government transitions
  - China as dominant party authoritarian regime

3. Four Generations of Controls in Cyberspace

Four Generations of Controls in Cyberspace (Deibert 2015)

- How do authoritarian states control and use cyberspace?
- First generation controls: Direct, defensive techniques such as Internet filtering
- Second generation controls: Legal measures extending to private sector
- Third generation controls: Offensive techniques such as directed attacks on civil society
- Fourth generation controls: Techniques for growing influence in Internet governance and taking control of own territorial cyberspace

Deibert, Ron. 2015. *Authoritarianism Goes Global: Cyberspace Under Siege*. Journal of Democracy, Volume 26, Number 3, July 2015, pp. 64-78. Last accessed on June 26, 2020. DOI: https://doi.org/10.1353/jod.2015.0051.
https://www.resurgentdictatorship.org/the-authoritarian-surge-into-cyberspace/

Driver of Authoritarianism in Cyberspace

- Why do authoritarian states control and use cyberspace?
  - New tool of regime survival
- Cause of authoritarian innovation in cyberspace: Serious concerns regarding cybercrime and terrorism, and governments' legitimate interest in combatting them
  - When democratic governments police cyberspace, it can have the effect of providing cover for authoritarian regimes to do the same for repression.
- "Big Brother" and "Big Data": Authoritarian demand for cybersecurity technology met by private firms
  - Economic efficiency rationale

Deibert, Ron. 2015. *Authoritarianism Goes Global: Cyberspace Under Siege*. Journal of Democracy, Volume 26, Number 3, July 2015, pp. 64-78. Last accessed on June 26, 2020. DOI: https://doi.org/10.1353/jod.2015.0051.
https://www.resurgentdictatorship.org/the-authoritarian-surge-into-cyberspace/

4. Findings on Turkey, Thailand, China, and Singapore

Turkey and Thailand

Turkey

Turkey

- Turkey has had the same dominant party regime since 2002.
- There had been significant curtailment of military influence.
  - Elections have been utilized as tools of legitimizing the actions of the government.
  - Public opinion is crucial for regime survival; while third generation of controls are becoming more common.

Turkey and Legal Authoritarianism

- BTK (Information Technologies and Communication Agency) : Access block on Wikipedia (2017-2020), YouTube (2007-8; 2010-11; 2011-2014), and Google Drive (2017) for 'national security' reasons
- Slander law: Slander against state leaders is punishable by imprisonment and/or monetary punishment
  - Used against political opponents
  - Twitter imprisonments, YouTube block also legitimized by slander laws
- New social media law in Turkey: Passed on July 30, 2020. Requires Internet providers to collect and report IP addresses on social media sites including port addresses to government
  - Local legal representative required for social media sites from June 2021 onwards
- AK Trolls: State-sponsored anonymous Internet political commentators and trolls recruited by the Justice and Development Party to push pro-gov narratives on social media and silence anti-gov ones
  - 2020 suspension of Twitter accounts of 7,340 users

https://www.btk.gov.tr/siber-guvenlik-kurulu
https://www.bbc.com/turkce/haberler-dunya-53581303

Thailand

Thailand

- With exceptions, Thailand has been ruled by military junta and military-backed civilian governments.
- Unless a civilian party gains majority, unelected senators appointed by the military elect the prime minister.
- The role of the monarchy, military, and civil society in recent requestioning

Thailand: Evolution of First Generation and Second Generation Controls

- Cybersecurity Act, B.E. 2562 (2019) published on 27 May 2019 and in effect now
- Private entities have obligations under two scenarios:

1. In an occurrence of cyber threats:

- (i) provide access to relevant computer data or a computer system, or other information related to the computer system only to the extent necessary to prevent cyber threats;
- (ii) monitor the computer or computer system; and
- (iii) allow officials to test the operation of the computer or computer system, or seize or freeze a computer, a computer system, or any equipment.
- Certain orders would require a court order, while others will not.

Thailand: Evolution of First Generation and Second Generation Controls

2. An organization which undertakes the following tasks or provide the following services are a Critical Information Infrastructure Organization (CII Organization):

(1) National security;

(2) Material public service;

(3) Banking and finance;

(4) Information technology and telecommunications;

(5) Transportation and logistics;

(6) Energy and public utilities;

(7) Public health;

(8) Others as prescribed by the National Cybersecurity Committee (NCSC)

Thailand: Evolution of First Generation and Second Generation Controls

- CII Organizations have compliance obligations:

(i) provide names and contact information of the owner(s), person(s) possessing the computer and person(s) monitoring the computer system;

(ii) comply with the code of practice and minimum cybersecurity standards;

(iii) conduct cybersecurity risk assessment; and

(iv) notify the authority of cyber threats.

- Penalties under the Act vary from fines to imprisonment.

Findings on Turkey and Thailand

- National security rhetoric. Regime survival is the primary concern.
- Application of first generation and second generation controls
  - Control of social media is the main method of control.
- Both regimes utilize second generation controls under basic level of legal authoritarianism.
- Their focus is not on decoupling their cyberspace from rest of the world, i.e. fourth generation controls.
  - A common mode of authoritarian state involvement in cyberspace
- Potential scaling down on authoritarian elements (via regime change, outside influence etc.) means potential scaling down on employment of controls
- Civilian authoritarianism and military-backed authoritarianism
  - As long as structures persist, first and second generation controls are expected to be prevalent.

China and Singapore

China

China

- Improved relations with ASEAN in the 1990's, member of BRICS
- Top trade partner for a number of countries
  - Well connected to world economy; greatest evidence is the economic slumps coinciding with world economy slumps
- China is a member of UN Security Council with a veto right but a non-influential or very latecomer member in other global institutions; does not lead any institution created under Bretton Woods system.
- AIIB and the OBOR Project: An alternative international financial/development system?
- Border and maritime disputes
- Political divergence from US-led world system: Norm differences becoming more visible in areas such as human rights and political representation

Efficiency in Economy and Political Control: China and FRP

- Since November 2018 (in effect since 2019), "all mobile phone users in China registering new SIM cards must submit to facial recognition scans."
- WeChat and AliPay using FRP: As of December 2019, "China's digital ID is integrated with popular online platform WeChat, allowing users to sync their national ID cards with the app and use their phones as IDs to buy train tickets or book hotels."
  - Facial-recognition payment (FRP, or "scan the face to pay", 刷脸支付)
- Ministry of Industry and Information gives the reasoning as a way to "protect the legitimate rights and interest of citizens in cyberspace"
  - Chinese mobile phone and internet users easier to track.

https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users#:~:text=All%20mobile%20phone%20users%20in,across%20the%20country%20on%20Sunday.&text=Many%20social%20media%20platforms%20also,identities%E2%80%9D%20via%20their%20phone%20numbers.
https://www.biometricupdate.com/201912/china-introduces-facial-recognition-for-wechat-transfers-mandatory-biometric-scans-for-sim-cards

The Great Firewall of China (防火长城)

- Combination of "firewall" and "the Great Wall of China"
  - First used in print by Geremie Barmé in 1997
- Formerly operated by the SIIO (predecessor of CAC) and since 2013 (in operation since 2014), operated by the Cyberspace Administration of China (CAC),
- CAC is described as being "in charge of translating the Communist Party of China's will into technical specifications."
- Internet censorship by blocking access to selected foreign websites, slowing down cross-border internet traffic, and requiring foreign companies to adapt to domestic regulations
  - Combination of all generations of controls except the third.
- Recent exclusion of Huawei hardware from Google Playstore means evolution of alternative software ecosystem closed off to outside world

"How China's Internet Police Control Speech on the Internet". Radio Free Asia. Archived from the original on 11 July 2013. Retrieved 15 August 2018.
Mozur, Paul; Goel, Vindu (5 October 2014). "To Reach China, LinkedIn Plays by Local Rules". The New York Times. Archived from the original on 13 June 2018. Retrieved 4 September 2017.

Singapore

Singapore

- Regional trade hub
- Technology and education leader in the region
- Founder member of ASEAN
- Small territory size and recent founding: Singapore is not a central player in global governance.

Tech-Savvy Legal Authoritarianism: Singapore

- Active state involvement in cyberspace
  - Engagement with the public via "gov.sg" involvement on social media channels
- Two key organizations:
  - New Defense Cyber Organization (DCO): Plans and implements policies in cyberspace (defense)
  - Cyber Security Agency (CSA): Prepares strategies for dealing with defacement of government websites
    - 2019 Report: Hacktivism included under criminal acts (Website Defacement Attacks)

https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019

Tech-Savvy Legal Authoritarianism: Singapore

- Internal Security Act (ISA) of Singapore: President can order detention to prevent subversion and anything incidental to internal security.
  - Detention without trial up to 2 years
  - Between 2002-2013, 64 'self-radicalized' people detained with viewing of online propaganda materials as evidence
- Cybersecurity Act: Cybersecurity regulator with power to investigate, seize evidence, and inflict criminal and civil penalties on noncompliers. Media also included in Critical Information Infrastructure (CII).
  - Requirement for CII owners to register for licenses
- Broadcasting Act: Any social media channel that handles transmission of news on Singaporean politics has to have a license
  - Prohibition from receiving foreign funding
- Cloud Software-as-a-Service (SaaS) Whitelisting: Compulsory for any firm offering cloud services to provide contractual details. Government may decide a firm is too risky

https://www.straitstimes.com/singapore/mda-asks-website-mothershipsg-to-register-under-broadcasting-act

Tech-Savy Legal Authoritarianism: Singapore

- First in the world to use facial verification in its national identity scheme
- Integration with SingPass for access to government and private sector services
  - iProov, a UK company providing the tech
  - Available to any business that wants it, and meets the government's requirements
  - "We don't really restrict how this digital face verification can be used, as long as it complies with our requirements," Kwok Quek Sin, senior director of national digital identity at GovTech Singapore

https://www.straitstimes.com/singapore/mda-asks-website-mothershipsg-to-register-under-broadcasting-act
https://www.bbc.com/news/business-54266602

Findings on China and Singapore

- Both globally connected in economic terms, mainly trade; not in terms of global governance
- Internal safety, ethnic harmony, and economic efficiency rationale rhetoric
- Systematic utilization of second generation of controls in a nuanced manner
- Differences in critical international pushback for employing controls
  - Especially in the case of Singapore, the tech-savvy government is praised
  - For Singapore, outright separation via fourth generation controls would cause economic losses as well international backlash
  - China is in the lead by effectively splitting its cyberspace from rest of the world.
  - Ongoing trade war creating incentives for Chinese companies to focus more on domestic market and create technologies for it

5. Conclusions

Conclusions

- 'Rule of law' subverted into 'rule by law'
  - Legal authoritarianism apparent in laws regarding cyberspace utilization in four cases
- Authoritarian regimes becoming more tech-savvy in their utilization of cyberspace
- First and basic second generation controls favored by more regime survival-focused authoritarian regimes
- Nuanced second generation and fourth generation controls favored by economically well connected but politically alternative authoritarian regimes

References

Cramer, Stella et al. . 2018. "Singapore's new Cybersecurity Act comes into force." In *Data Protection Report.* Norton Rose Fulbright. Last accessed on November 10, 2020: https://www.dataprotectionreport.com/2018/09/singapores-new-cybersecurity-act-come-into-force-heres-what-you-need-to-know/#:~:text=The%20much%20discussed%20Cybersecurity%20Act,31%20August%202018%20%5B1%5D.&text=It%20also%20creates%20a%20licensing,in%20Singapore%20to%20be%20registered.

Deibert, Ron. 2015. "Authoritarianism Goes Global: Cyberspace Under Siege." In *Journal of Democracy*, vol. 26 no. 3, 2015, p. 64-78. Project MUSE, doi:10.1353/jod.2015.0051.

Farrell, Henry and Newman, Abraham L. . 2020. "Chained to Globalization: Why It's Too Late to Decouple." In *Foreign Affairs,* January/February 2020. Last accessed on November 10, 2020: https://www.foreignaffairs.com/articles/united-states/2019-12-10/chained-globalization

Cimpanu, Catalin. 2020. *EU sanctions China, Russia, and North Korea for past hacks*. Last accessed on November 10, 2020: https://www.zdnet.com/article/eu-sanctions-china-russia-and-north-korea-for-past-hacks/.

Cimpanu, Catalin. 2020. *DEF CON: New tool brings back 'domain fronting' as 'domain hiding'.* Last accessed on November 10, 2020: https://www.zdnet.com/article/def-con-new-tool-brings-back-domain-fronting-as-domain-hiding/.

Cimpanu, Catalin. 2020. *Iranian hackers restart attacks on universities as the new school year begins*. Last accessed on November 10, 2020: https://www.zdnet.com/article/iranian-hackers-restart-attacks-on-universities-as-the-new-school-year-begins/.

Ponniah, Kevin. 2020. *How a Chinese agent used LinkedIn to hunt for targets*. BBC News. Last accessed on November 10, 2020: https://www.bbc.com/news/world-asia-53544505.

Singpeng, Aim. 2017. *Divide and Conquer: Authoritarianism and Cyberspace in Southeast Asia*. Last accessed on November 10, 2020: https://international.thenewslens.com/article/82673.

Southeast Asian Press Alliance (SEAPA). 2019. *Singapore: Cyberspace Headed for More Control*. Last accessed on November 10, 2020: https://old.pcij.org/stories/singapore-cyberspace-headed-for-more-control/.

Suwanprateep , Dhiraphol. 2019. *Thailand Cybersecurity Act is Effective* . Baker McKenzie. Last accessed on November 10, 2020: https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-cybersecurity-act-is-effective.

Thank you for listening.