IIC 2022

ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

The 2nd International Conference on Advanced Technology and Sustainable Development - 2022 (ICATSD2022)

Plenary session PRESENTATION

November 24-26, 2022

Organized by
Industrial University of Ho Chi Minh City & Eastern International University
Vietnam

ICATSD 2022

The 2nd International Conference on Advanced Technology
& Sustainable Development - ICATSD 2022

INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

EIU

CỤC CÔNG TÁC PHÍA NAM

CONFERENCE AGENDA

THE 2nd INTERNATIONAL CONFERENCE ON ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT - 2022 (ICATSD2022)

Friday, November 25, 2022

Venue: Industrial University of Ho Chi Minh City

Time	Event and Place
8.00 – 8.30	**Conference Registration Opening – Building E**
8.30-8.45	**Performance**
8.45 - 10.45	**PLENARY SESSION – Conference Hall E.4, Building E**
8.45-9.00	**Conference Opening**
9.00-9.20	**Welcome Speeches** - *Dr. Phan Hong Hai – Rector of Industrial University of Ho Chi Minh City;* - *Dr. Ngo Minh Duc – Rector of Eastern International University;* - *Mr. Nguyen Manh Cuong – Deputy Director General of Agency for Southern Affair of Ministry of Science and Technology* - *Dr. Le Thanh Minh – Deputy Director of Ho Chi Minh City Department of Science and Technology*
9.20-10.30	**Keynote Speaker 1** ***Prof. Marco Abbiati****, University of Bologna, Science Attaché at the Italian Embassy in Hanoi, Vietnam* **Keynote Speaker 2** ***Prof. Tsan-Ming Choi (Jason****), University of Liverpool Management School, UK* **Keynote Speaker 3** ***Assoc. Prof. John Luke Gallup****, Portland State University, Portland, USA* **Conference Chair** ***Prof. Le Van Tan****, Industrial University of Ho Chi Minh City* ***Prof. Fabien De Geuser****, CFVG, French Vietnamese School of Management, ESCP Europe*
10.30-10.45	**Tea break, Photographs and Transfer to Symposiums Session**
10.45 - 12.00	**SYMPOSIUMS SESSION**
10.45- 12.00	***1. The 2022 International Conference on Computational Intelligence and Innovative Applications 2022 (CIIA 2022):*** *Place: Room B4.5, Building B (as the CIIA agenda attached)* ***2. The International Symposium on Precision Machining and Advanced Technologies (ISPMAT 2022):*** *Place: Room B4.6, Building B (as the ISPMAT agenda attached)*

	3. The International Symposium for Green Solutions (ISGS 2022): *Place: Research Room 1 & Research Room 3 (as the ISGS agenda attached)* ***4. The International Symposium on Sustainable Development in Transition Economies 2022 (ISSDTE 2022):*** *Place: Room meeting E4, Building E (as the ISSDTE agenda attached)* ***5. The International Symposium on Innovations and Sustainable Development in Social Sciences and Humanities (ISDSSH 2022)*** *Place: Room meeting E3.2, Building E (as the ISDSSH agenda attached)*
12.00-13.00	**Lunch break**
13.00- 14.00	**POSTER SESSION – The Hall Building H**
14.00- 16.00	**SYMPOSIUMS SESSION (continued)** ***1. The 2022 International Conference on Computational Intelligence and Innovative Applications 2022 (CIIA 2022):*** *Place: Room B4.2, B4.3, B4.4, B4.5 - Building B (as the CIIA agenda attached)* ***2. The International Symposium on Precision Machining and Advanced Technologies (ISPMAT 2022):*** *Place: Room B4.6, B4.7, B4.8, B4.9 - Building B (as the ISPMAT agenda attached)* ***3. The International Symposium for Green Solutions (ISGS 2022):*** *Place: Research Room 1 & Research Room 3 (as the ISGS agenda attached)* ***4. The International Symposium on Sustainable Development in Transition Economies 2022 (ISSDTE 2022):*** *Place: Room meeting E4, Building E (as the ISSDTE agenda attached)* ***5. The International Symposium on Innovations and Sustainable Development in Social Sciences and Humanities (ISDSSH 2022)*** *Place: Room meeting E3.2, Building E (as the ISDSSH agenda attached)*
16.00-16.15	**Tea break and Transfer to Closing Session**
16.15- 16.40	**CLOSING SESSION – Conference Hall E.4**
16.15-16.20	**Closing Ceremony** ***Assoc. Prof. Dam Sao Mai****, Industrial University of Ho Chi Minh City*
16.20-16.40	**Poster and Oral Presentation Awards**
17.30-21.00	**GALA DINNER – Luxury Restaurant, No. 171 Nguyen Thai Son Street, Go Vap District, Ho Chi Minh City**
17.30-18.00	**Registration**
18.00-21.00	• **Welcome and Opening Remarks** • **Dinner**

Saturday, November 26, 2022 TECHNICAL TOUR Place: Binh Duong Province	
Time	**Event and Place**
8.00-8.30	**Registration** **Venue: Industrial University of Ho Chi Minh City**
8.30-10.00	**Departure to VSIP Industry Parts, Binh Duong Province**
10.00-11.45	• **Visit VSIP Headquarters – Presentation of VSIP Group history & milestones, projects, tenants' products & services and 3D model of VSIP III.** • **Visit a tenant in VSIP I - Corporate social responsibility** (ISSDTE2022 & ISDSSH2022), **Advanced manufacturing systems** (CIIA2022, ISPMAT2022 & ISGS2022) • **Visit Binh Duong New City – Becamex Tokyu HQ: - Sustainable and smart region development (Bus tour: Administration & Exhibition Center, WTC, Tokyu Garden City, Central Park, EIU)**
12.00-13.00	**Networking and Lunch at Becamex Hotel – Becamex IDC**
13.00-14.00	**Return to Ho Chi Minh City**

Marco Abbiati

Prof Marco Abbiati, PhD Science and Technology Counsellor - Embassy of Italy to Vietnam, Hanoi, Vietnam
Department of Cultural Heritage, Ravenna Campus, Alma Mater Studiorum – University of Bologna, Italy

Marco Abbiati main research interests are sustainable development and long-term management of natural resources, with a focus marine habitats. He applies a multidisciplinary approach to investigate ecosystem functioning, biodiversity conservation, climate change mitigation and resilience, impact of pollution. He has been visiting scientist at Sydney University, UCSC, Moscow Academy of Science, University of Adelaide, Wesleyan University, and coordinated several research projects addressing fundamental and applied research founded by the EU Framework Programmes, Italian Ministries and private enterprises. In Vietnam he collaborates with Vietnamese Universities and Academies, Ministries and UN Agencies to promote Italian-Vietnamese and multilateral partnerships in science and technology. He is author and co-author of more the 100 peer-reviewed papers, book chapters and of numerous presentations to national and international conferences.

IIC 2022
ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

INDUSTRIAL
UNIVERSITY OF
HOCHIMINH CITY

EIU

CỤC CÔNG TÁC PHÍA NAM

The 2nd International Conference on Advanced Technology
& Sustainable Development (ICATSD 2022)

Sustainability and new technologies in blue economy: can a balance be found?

Marco Abbiati[1,2]

[1] Science and Technology Counsellor, Embassy of Italy to Vietnam

[2] Professor of Environmental Sciences, Alma Mater Studiorum-University of Bologna, Italy

marco.abbiati@esteri.it
marco.abbiati@unibo.it

CONTENTS

01 Understanding Well Being

02 Defining Sustainable Development

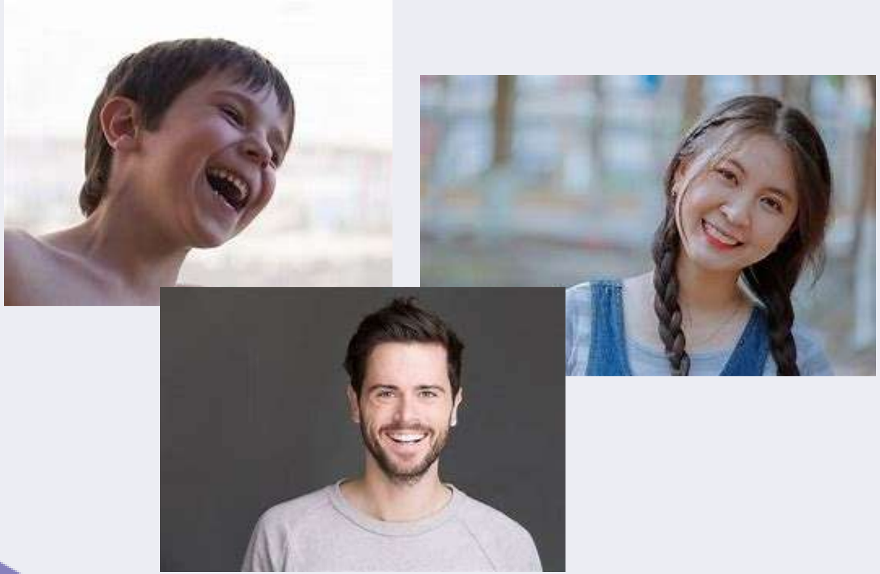
03 Good or Bad Technology?

04 Some Examples

05 Where To Go NBSs

Understanding well being

From Happiness to Prosperity: a shift in importance



Not Resource Intensive

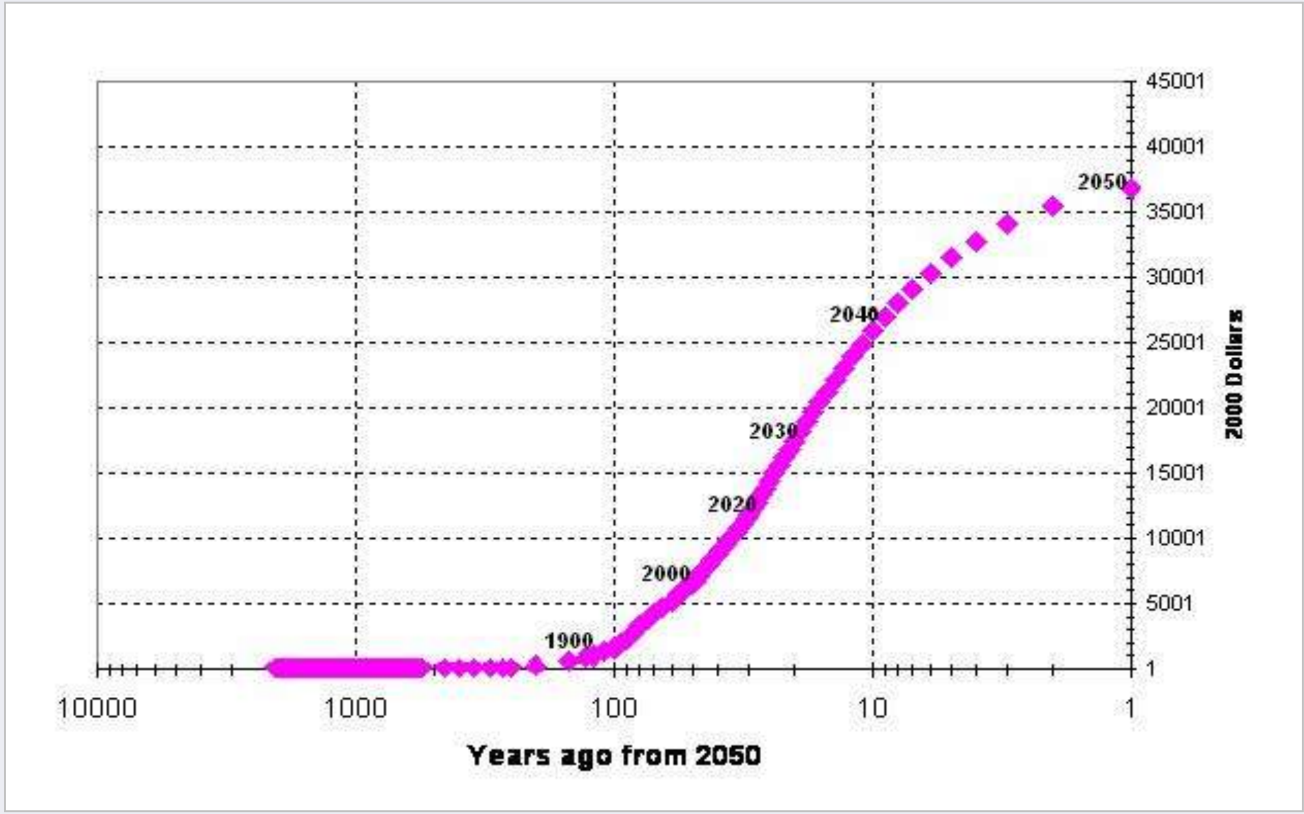
Resource Intensive

Resource Utilization

Resource Exploitation

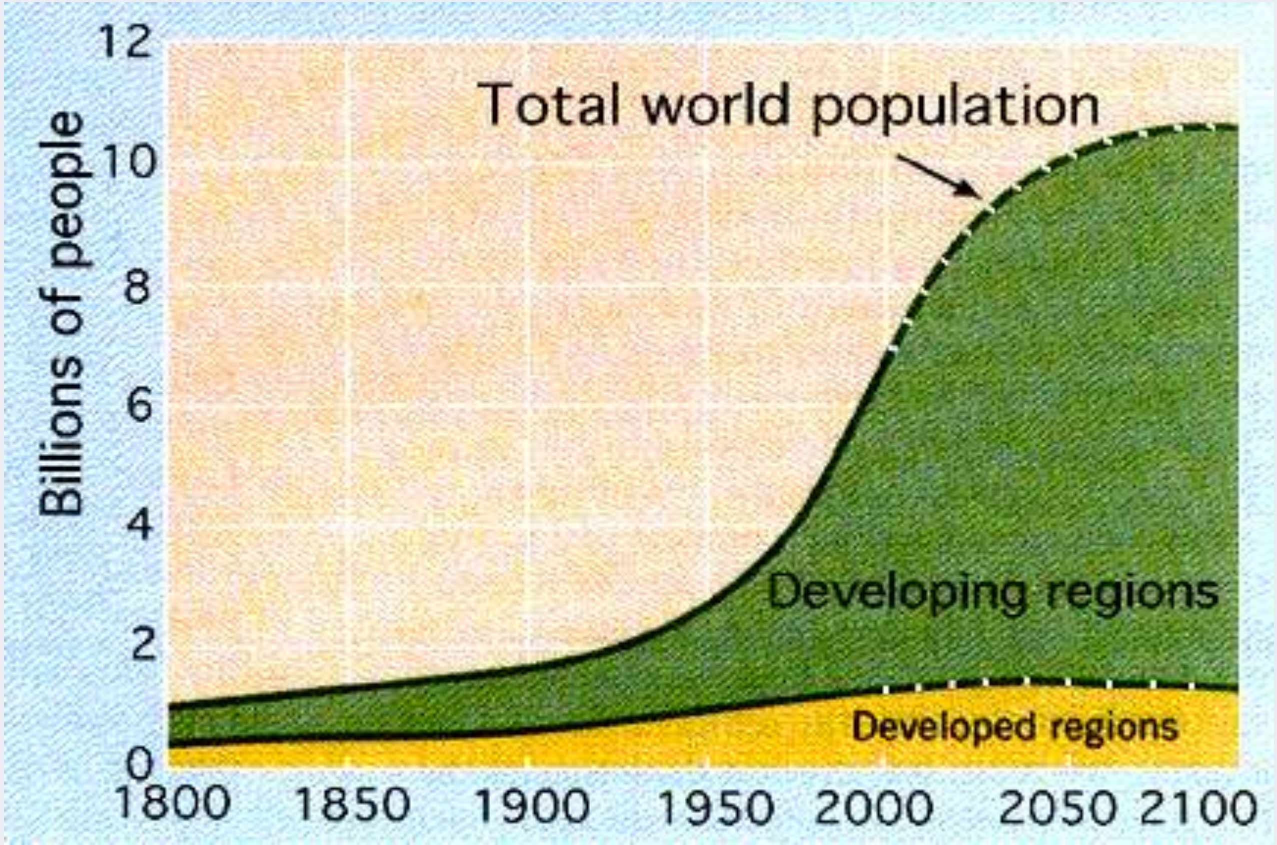
Understanding well being

World Per Capita GDP



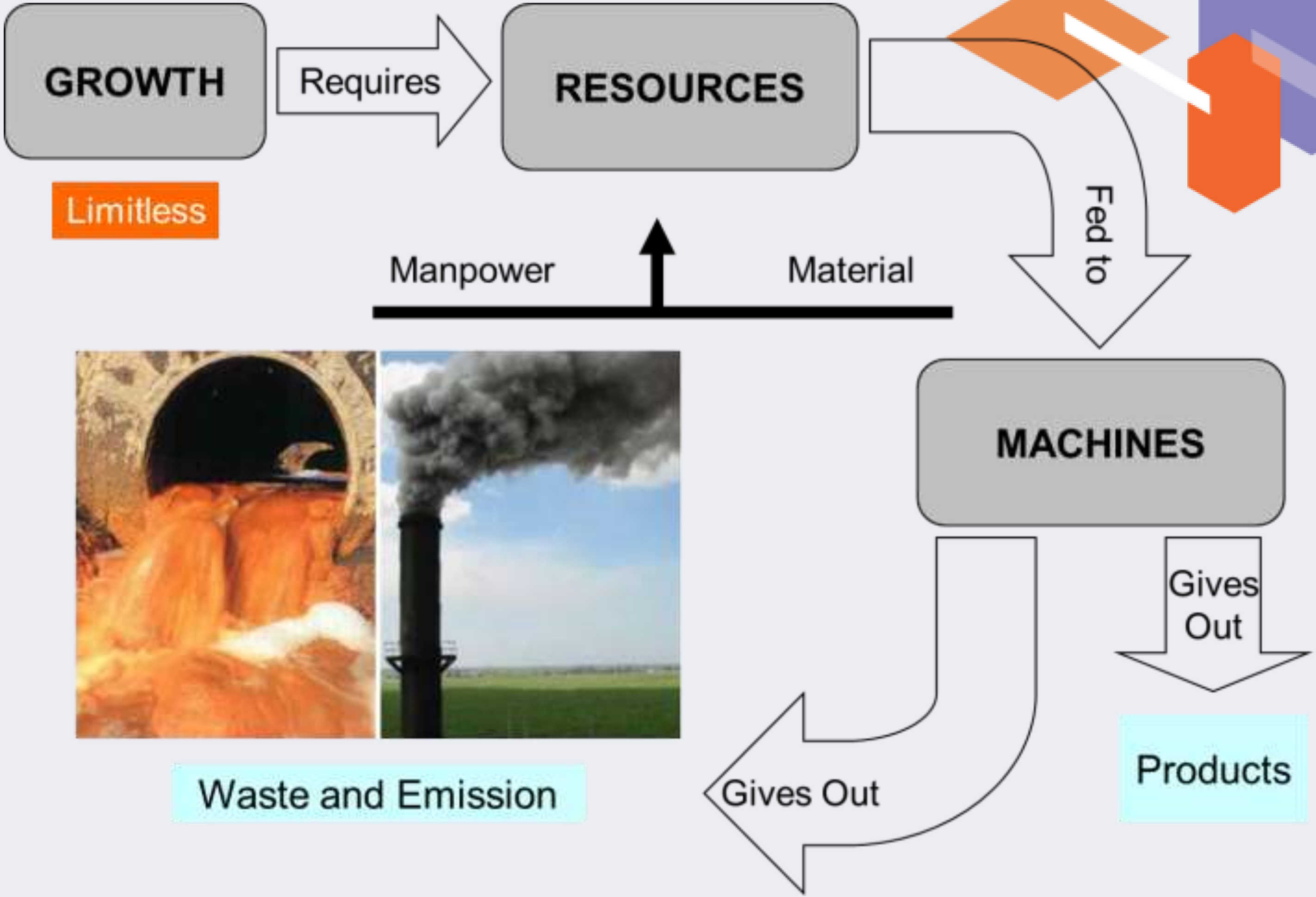
Understanding well being

Population Growth



Understanding well being

Waste and Emissions



GROWTH

Requires

RESOURCES

Limitless

Manpower

Material

Fed to

MACHINES

Gives Out

Products

Gives Out

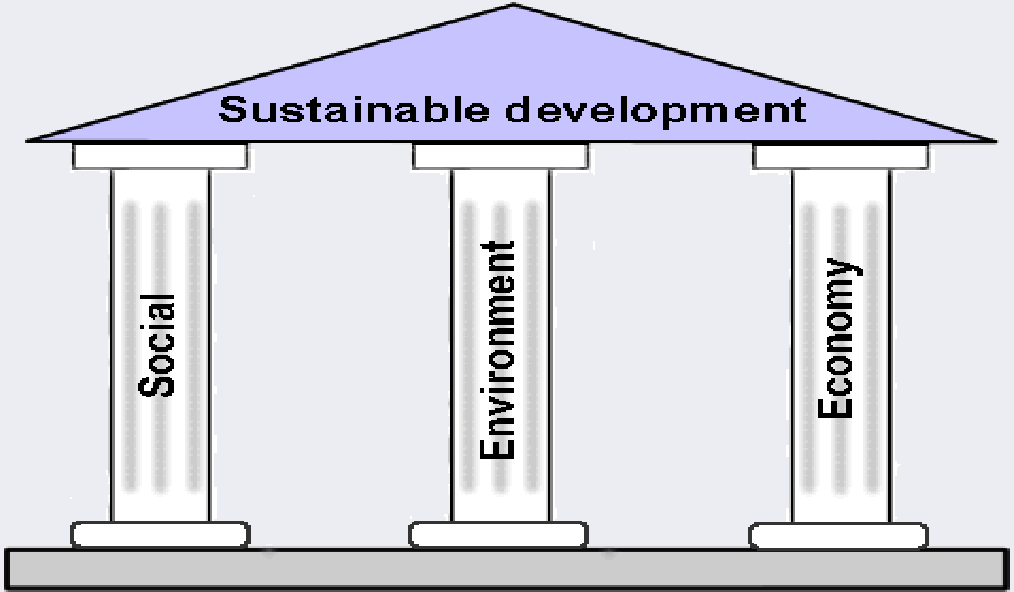
Waste and Emission

Sustainable Development

Brundtland Commission Rio 1987

SD define as

Development that **meets the needs of the present** without compromising the ability of future generations **to meet their own needs**



Good or Bad Technologies?

S&T for sustainable well-being

Science:

improving understanding of threats & possibilities

enabling advances in technology

Technology:

driving economic growth via new products & services, reduced costs, increased productivity

<u>reducing resource use & environmental impacts</u>

S&T:

integrated assessment of options

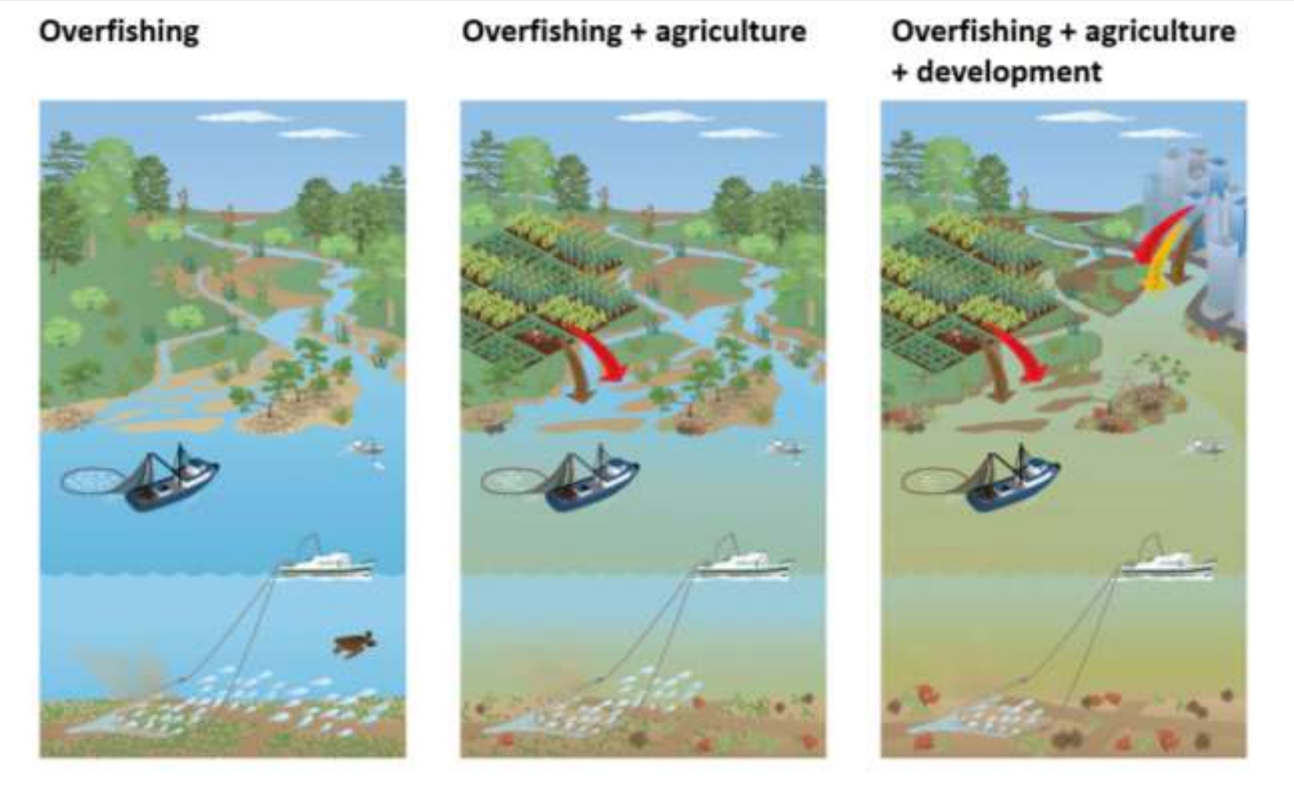
advice to decision-makers & the public about costs, benefits, dangers, uncertainties

S&T education toward a more S&T-literate society

New Technologies

They can **drive resource exploitation**

In coastal habitat



Overfishing

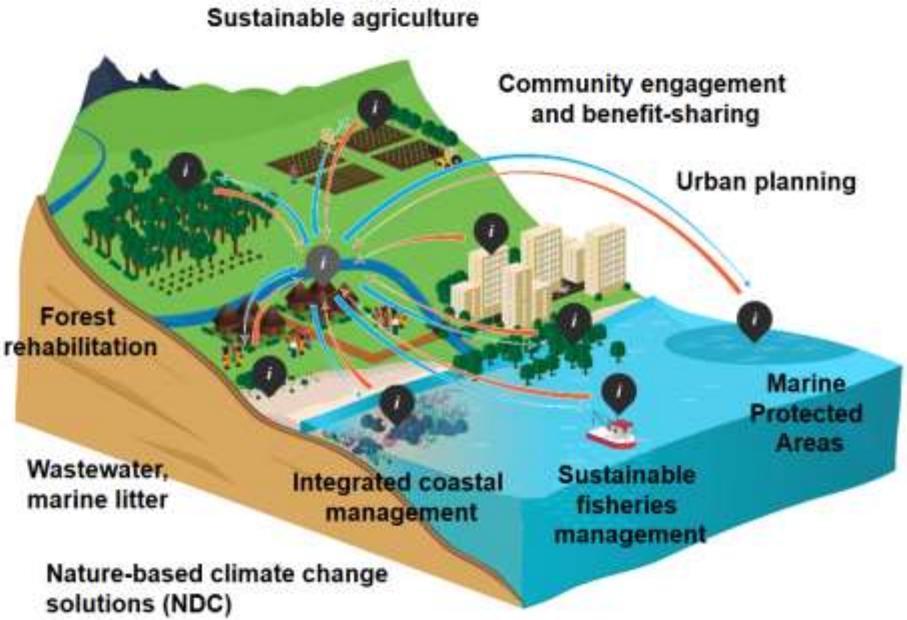
Overfishing + agriculture

Overfishing + agriculture + development

New Technologies

or they can **optimize resource exploitation**

In coastal habitat

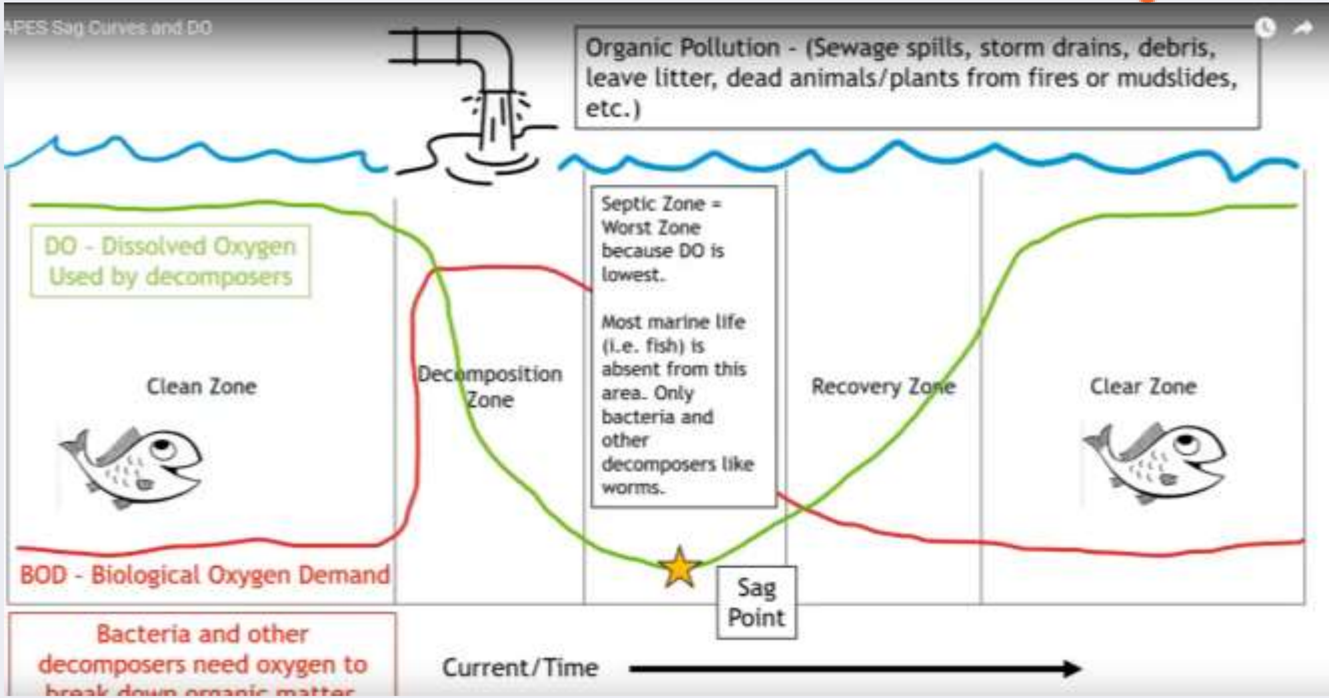

Sustainable agriculture
Community engagement and benefit-sharing
Urban planning
Forest rehabilitation
Marine Protected Areas
Wastewater, marine litter
Integrated coastal management
Sustainable fisheries management
Nature-based climate change solutions (NDC)

- Optimal use of ocean space and services
- Reduced land-based impacts on coastal natural capital
- Enhancing resource efficiency and economic circularity
- Reduce climate vulnerabilities & risks to protect infrastructures and economies
- Innovative financing

How We Use Technologies?

Wastewater pollution

From free ecosystem service to pollution



Organic Pollution - (Sewage spills, storm drains, debris, leave litter, dead animals/plants from fires or mudslides, etc.)

Septic Zone = Worst Zone because DO is lowest.

Most marine life (i.e. fish) is absent from this area. Only bacteria and other decomposers like worms.

Bacteria and other decomposers need oxygen to break down organic matter

How We Use Technologies?

Wastewater treatment

Exclusively technologic solution

How We Use Technologies?

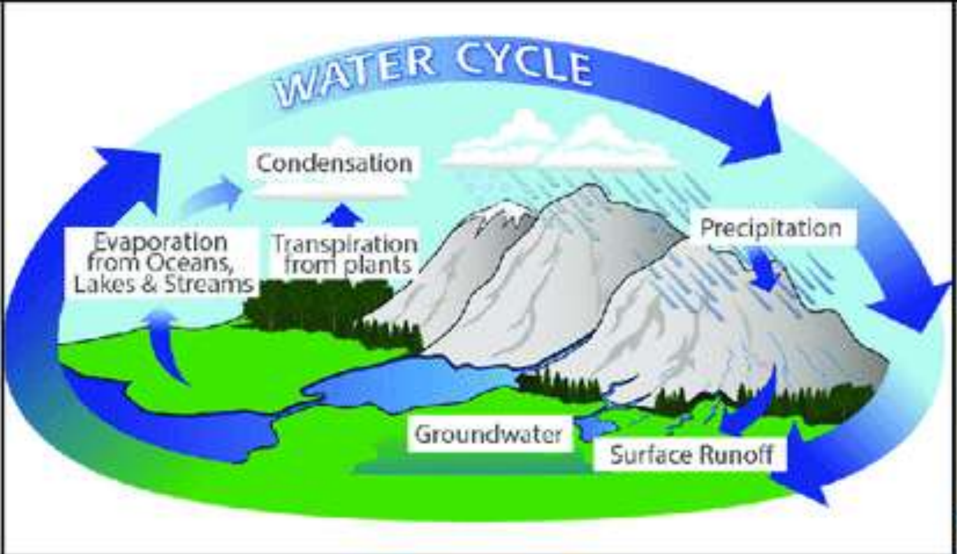
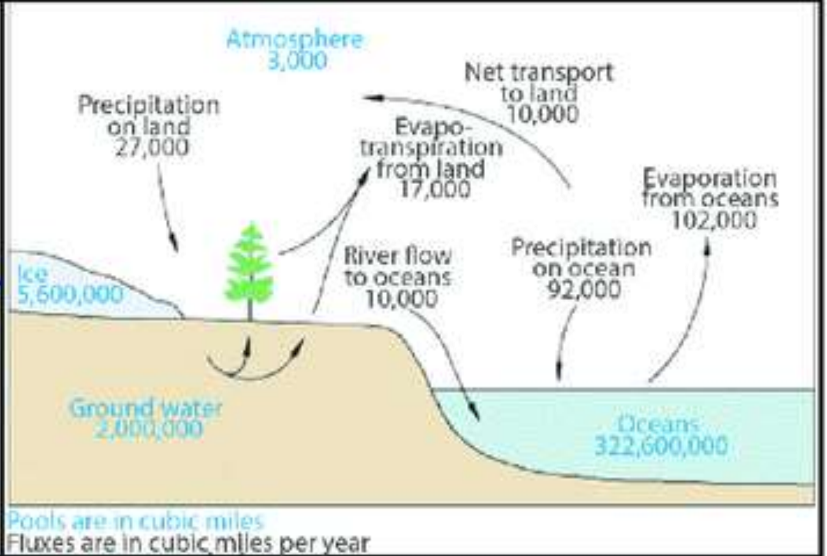
Waste water treatment

Technology using natural processes

Circular processes

Learning form nature: **water, N, C, P, S …**

Bio-geo-chemical cycles

	CYCLE	BUDGET
GLOBAL		

WATER CYCLE
Condensation
Evaporation from Oceans, Lakes & Streams
Transpiration from plants
Precipitation
Groundwater
Surface Runoff

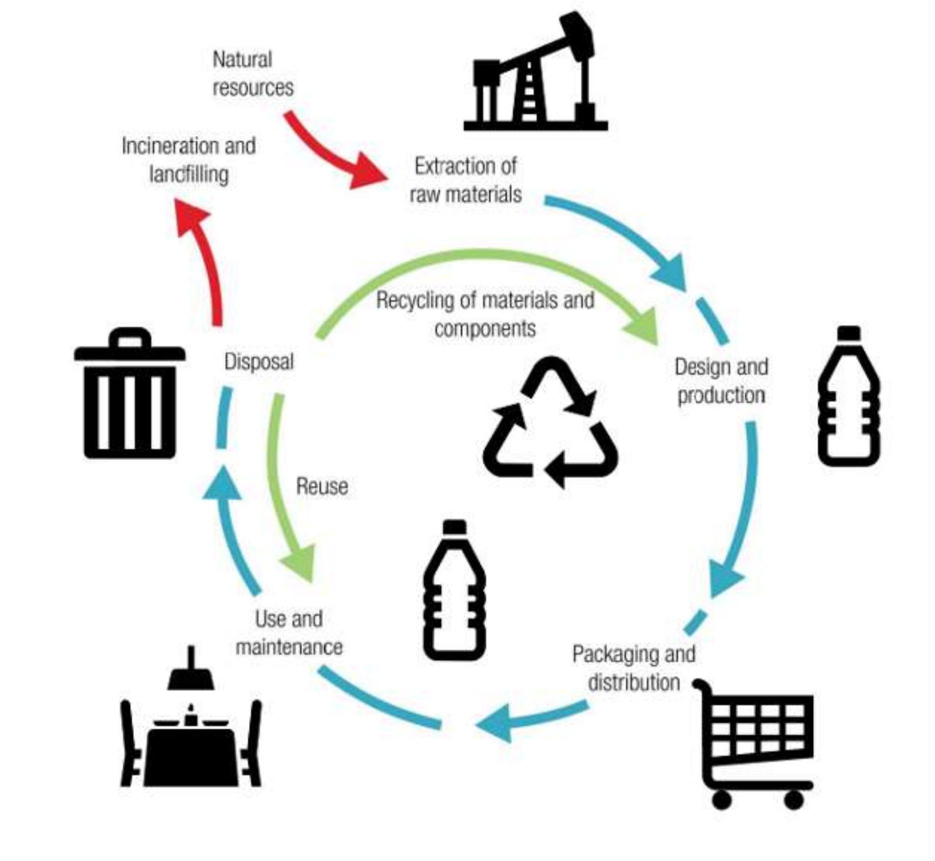
Atmosphere 3,000
Precipitation on land 27,000
Net transport to land 10,000
Evapo-transpiration from land 17,000
Evaporation from oceans 102,000
Ice 5,600,000
River flow to oceans 10,000
Precipitation on ocean 92,000
Ground water 2,000,000
Oceans 322,600,000

Pools are in cubic miles
Fluxes are in cubic miles per year

Circular processes

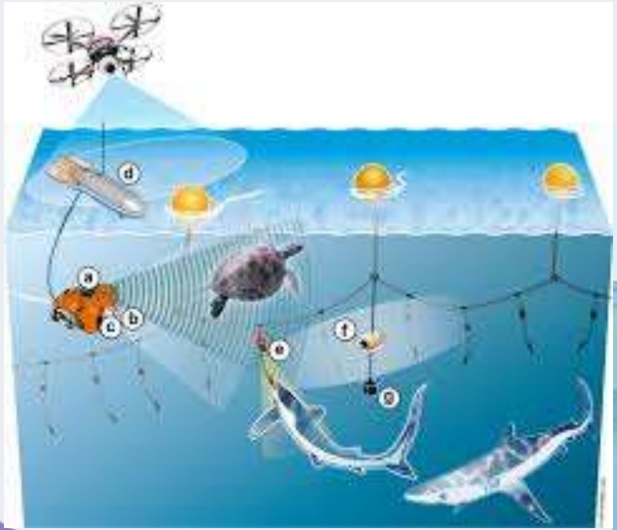
Circular economy

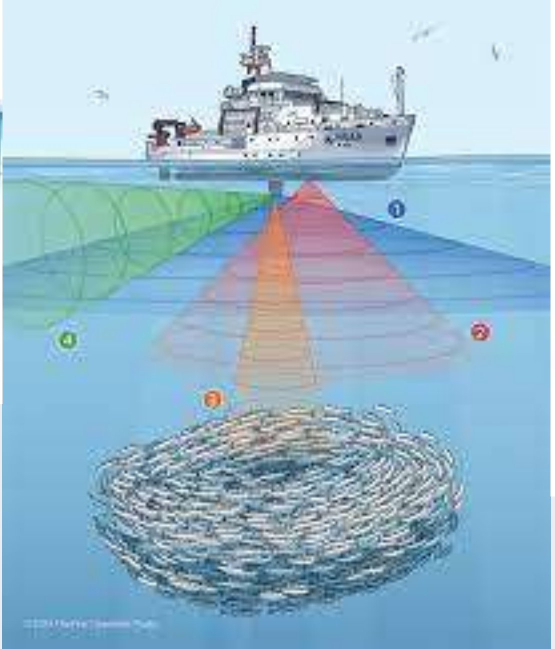
The plastic issue

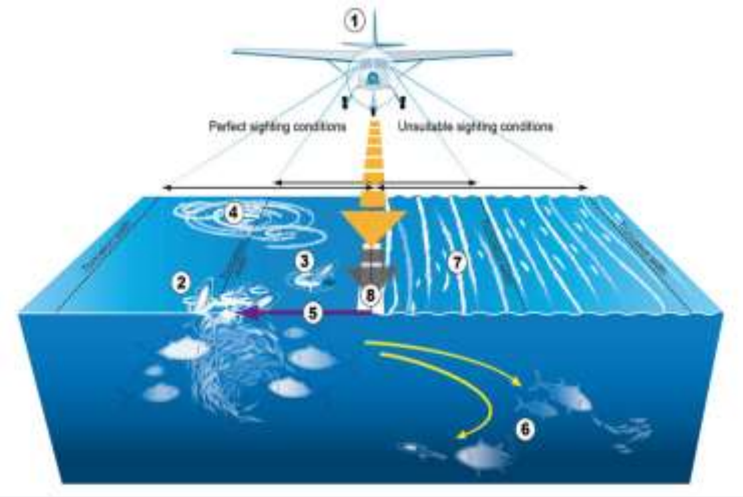

Natural resources
Extraction of raw materials
Design and production
Packaging and distribution
Use and maintenance
Disposal
Incineration and landfilling
Recycling of materials and components
Reuse

Technologies for fisheries

New tools for a more effective harvest







New technologies

Monitoring and conservation

PML
AutoNaut

Coastal Defense Technologies

Gray traditional infrastructures

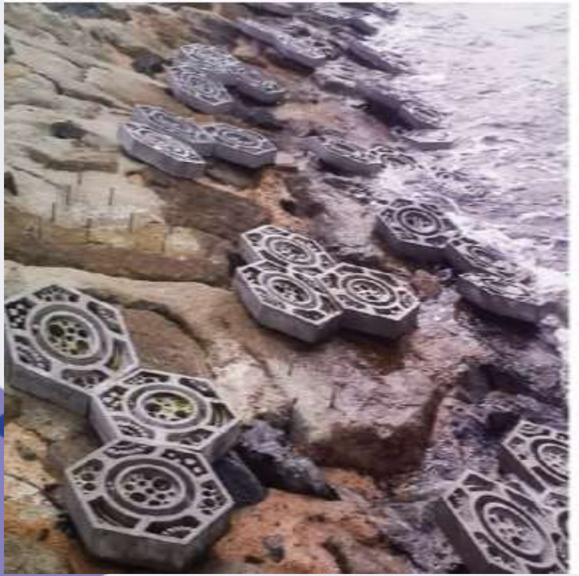
- High environmental impacts
- Poor ecological performance
- High Carbon footprint
- High costs

Coastal Defense Technologies

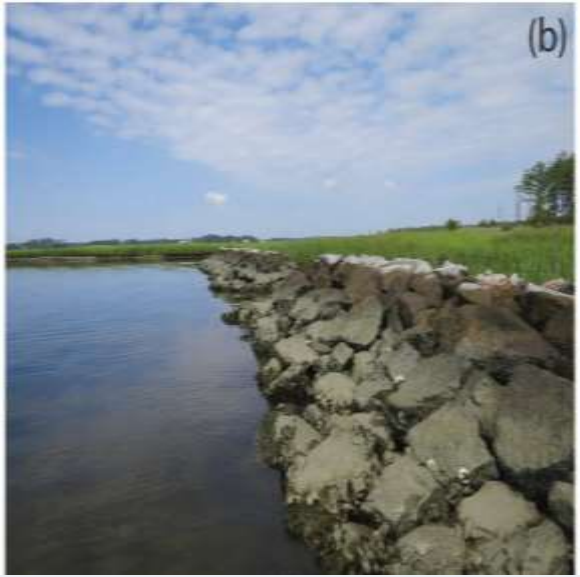
Greener technological solutions

S&T can help!

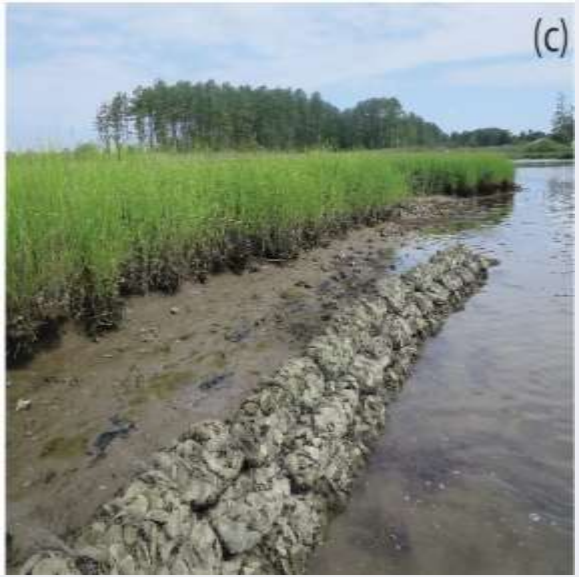
Greening gray infrastructure



Hybrid projects



Soft restoration

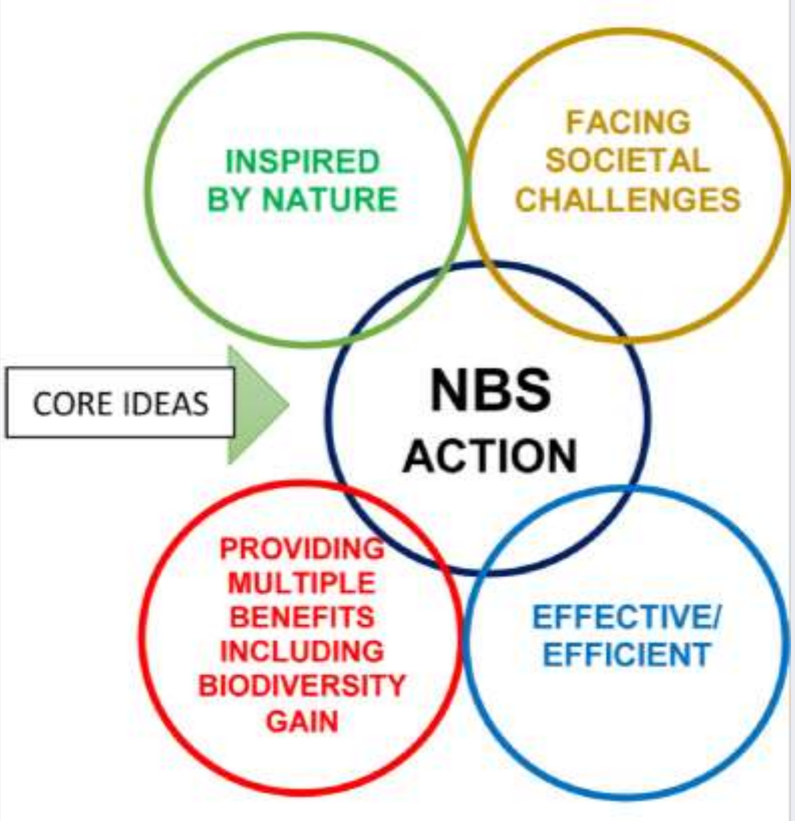


Where to go? NBSs - Nature Based Solutions

Science and Technology working with Nature

Term first used in 2008 by the World Bank

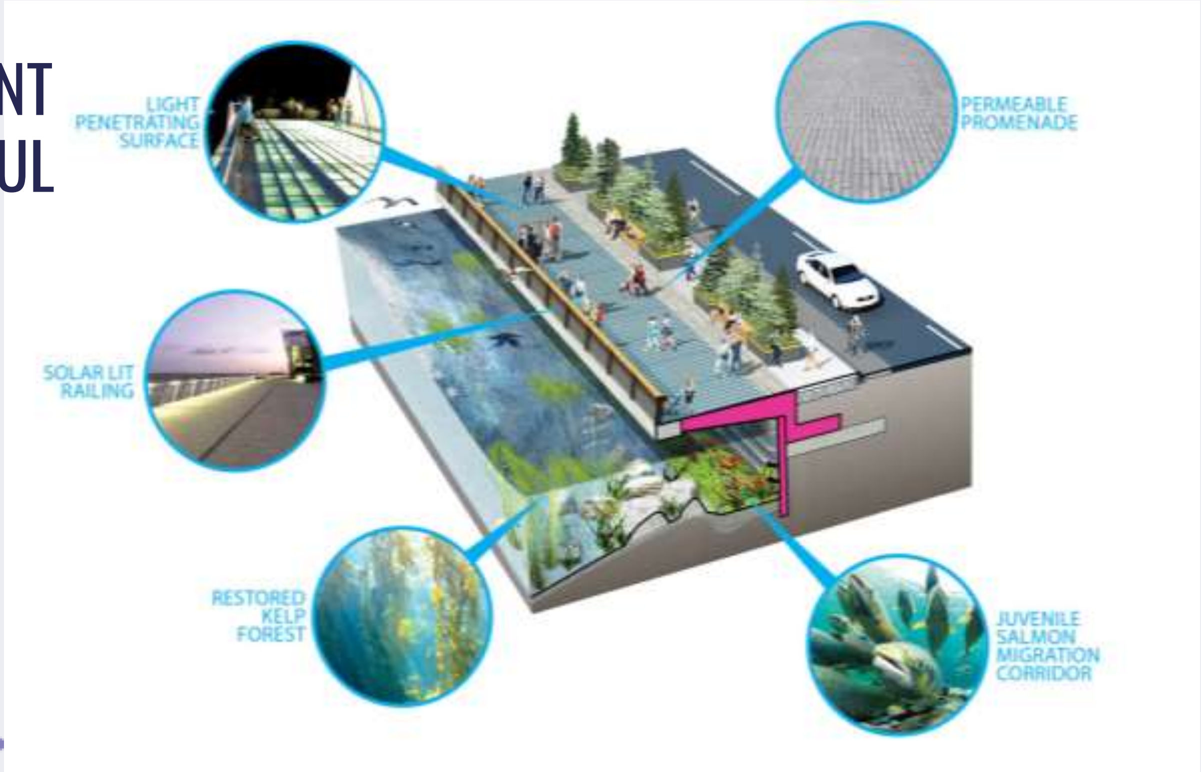
It refers to the sustainable management and use of natural features and processes to tackle socio-environmental challenges


CORE IDEAS
INSPIRED BY NATURE
FACING SOCIETAL CHALLENGES
NBS
ACTION
PROVIDING MULTIPLE BENEFITS INCLUDING BIODIVERSITY GAIN
EFFECTIVE/ EFFICIENT

Nature Based Solutions

Science:

SEATTLE WATERFRONT A SUCCESFUL EXAMPLE



Where to go?

Establish clear links between design, ‘novel’ biodiversity and desired services

HOW TO FURTHER IMPROVE?

[illegible]

Contents lists available at ScienceDirect

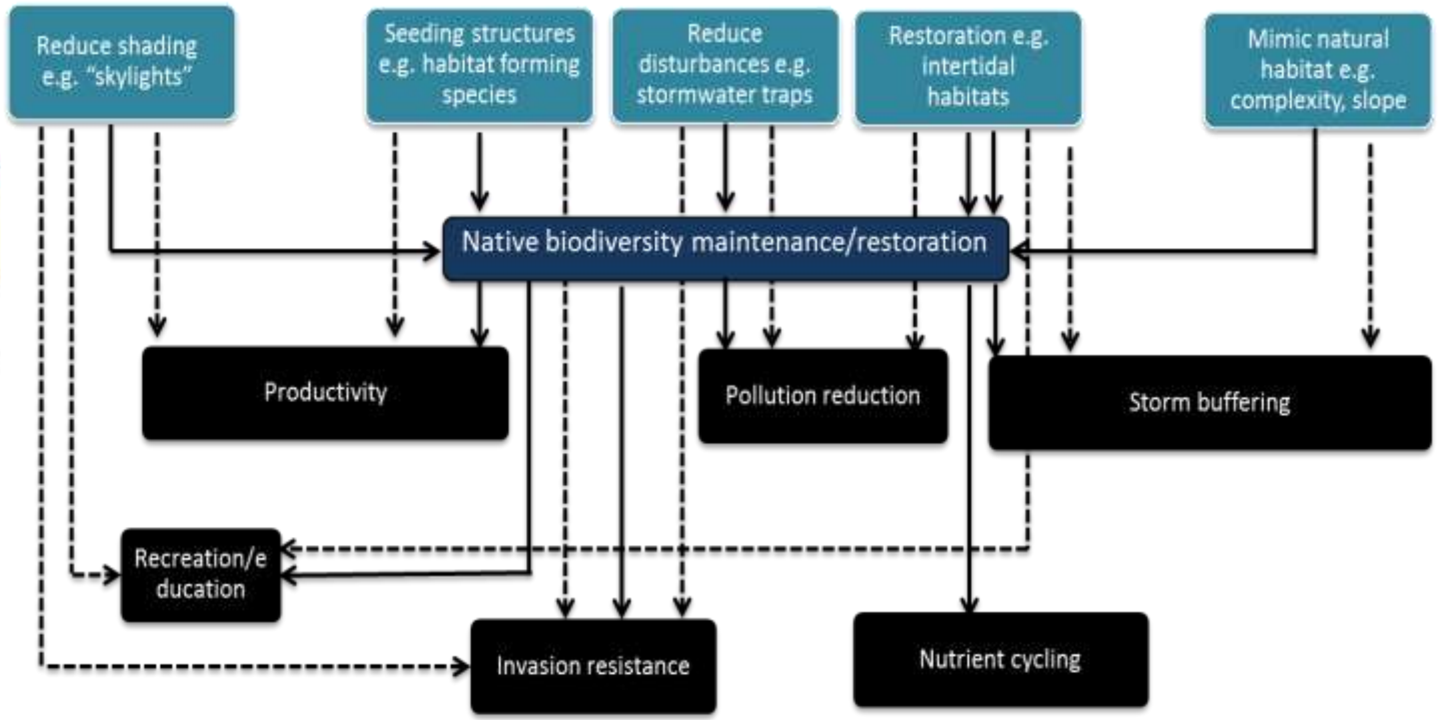
Journal of Environmental Management

journal homepage: www.elsevier.com/locate/jenvman

Discussion

Building ‘blue’: An eco-engineering framework for foreshore developments

M. Mayer-Pinto [a,b,*], E.L. Johnston [a,b], A.B. Bugnot [a,b], T.M. Glasby [c], L. Airoldi [d], A. Mitchell [e], K.A. Dafforn [a,b]



Reduce shading e.g. “skylights”
Seeding structures e.g. habitat forming species
Reduce disturbances e.g. stormwater traps
Restoration e.g. intertidal habitats
Mimic natural habitat e.g. complexity, slope
Native biodiversity maintenance/restoration
Productivity
Pollution reduction
Storm buffering
Recreation/education
Invasion resistance
Nutrient cycling

I wish to thank you for your time

Tsan-Ming CHOI (Jason), PhD

Tsan-Ming CHOI (Jason) is currently Chair in Operations and Supply Chain Management, and Director of the Centre for Supply Chain Research at University of Liverpool Management School (ULMS). He has published extensively in leading journals in the fields of operations management, engineering management, logistics and supply chain management. He is currently serving the profession as the Co-Editor-in-Chief of Transportation Research Part E: Logistics and Transportation Review, a Department Editor of IEEE Transactions on Engineering Management, a Senior Editor of Production and Operations Management, and Decision Support Systems, and an Associate Editor of Decision Sciences, and IEEE Transactions on Systems, Man and Cybernetics - Systems. He is also a member of the Engineering Panel of Research Grants Council of Hong Kong. His current research interests include the use of blockchain for supply chain management and he is chairing a related special interest group (SiG) under IEEE Technology and Engineering Management Society (IEEE-TEMS). Before joining ULMS in September 2022, he taught at The Chinese University of Hong Kong, The Hong Kong Polytechnic University, and National Taiwan University together for over twenty years.

IIC2022
ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

INDUSTRIAL
UNIVERSITY OF
HOCHIMINH CITY

EIU

CỤC CÔNG TÁC PHÍA NAM

The 2nd International Conference on Advanced Technology
& Sustainable Development (ICATSD 2022)

E-Commerce Supply Chains with Considerations of Cyber-Security: Roles of Governments and Blockchain Technologies

Tsan-Ming CHOI (Jason), PhD

Chair in Operations and Supply Chain Management, and

Director of Centre for Supply Chain Research,

University of Liverpool Management School

25 November, 2022

References

- This talk is based on my following two recently published POM papers:
    - Choi, T.M., S. Kumar, X. Yue, H.L. Chan. Disruptive technologies and operations management in the Industry 4.0 era and beyond. *Production and Operations Management*, 31(1), 9-31, 2022.
        - **Industry 5.0: Sustainable social welfare.**
    - Luo, S., T.M. Choi. E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Production and Operations Management*, 31 (5), 2107-2126, 2022.

VOLUME 31 | NUMBER 3 | MARCH 2022

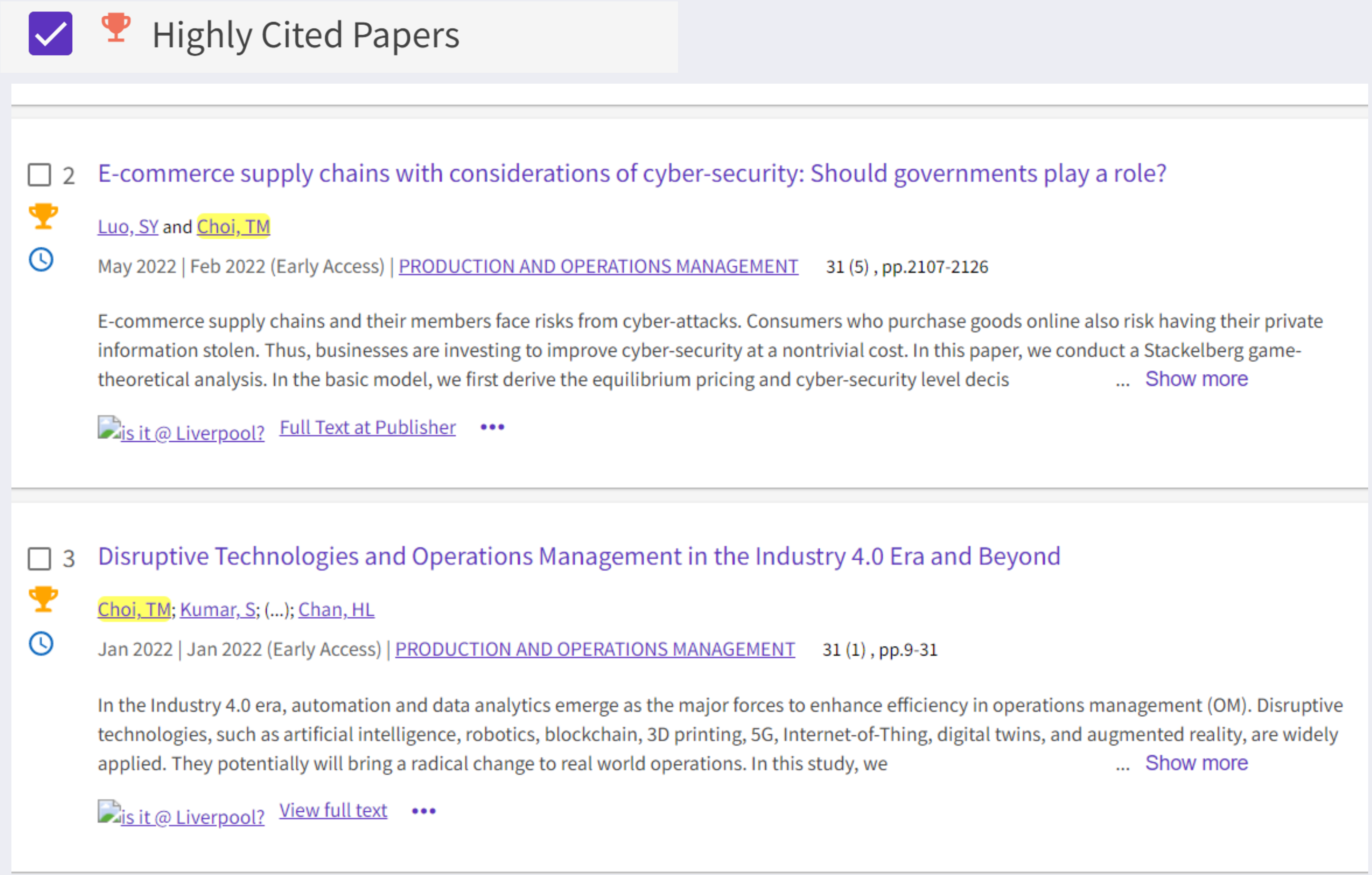
PRODUCTION AND OPERATIONS MANAGEMENT

WILEY

THE FLAGSHIP RESEARCH JOURNAL OF PRODUCTION AND OPERATIONS MANAGEMENT SOCIETY

POMS

Web of Science: Highly cited



☑ 🏆 Highly Cited Papers

□ 2 E-commerce supply chains with considerations of cyber-security: Should governments play a role?

🏆 Luo, SY and Choi, TM

May 2022 | Feb 2022 (Early Access) | PRODUCTION AND OPERATIONS MANAGEMENT 31 (5) , pp.2107-2126

E-commerce supply chains and their members face risks from cyber-attacks. Consumers who purchase goods online also risk having their private information stolen. Thus, businesses are investing to improve cyber-security at a nontrivial cost. In this paper, we conduct a Stackelberg game-theoretical analysis. In the basic model, we first derive the equilibrium pricing and cyber-security level decis ... Show more

is it @ Liverpool? Full Text at Publisher •••

□ 3 Disruptive Technologies and Operations Management in the Industry 4.0 Era and Beyond

🏆 Choi, TM; Kumar, S; (...); Chan, HL

Jan 2022 | Jan 2022 (Early Access) | PRODUCTION AND OPERATIONS MANAGEMENT 31 (1) , pp.9-31

In the Industry 4.0 era, automation and data analytics emerge as the major forces to enhance efficiency in operations management (OM). Disruptive technologies, such as artificial intelligence, robotics, blockchain, 3D printing, 5G, Internet-of-Thing, digital twins, and augmented reality, are widely applied. They potentially will bring a radical change to real world operations. In this study, we ... Show more

is it @ Liverpool? View full text •••

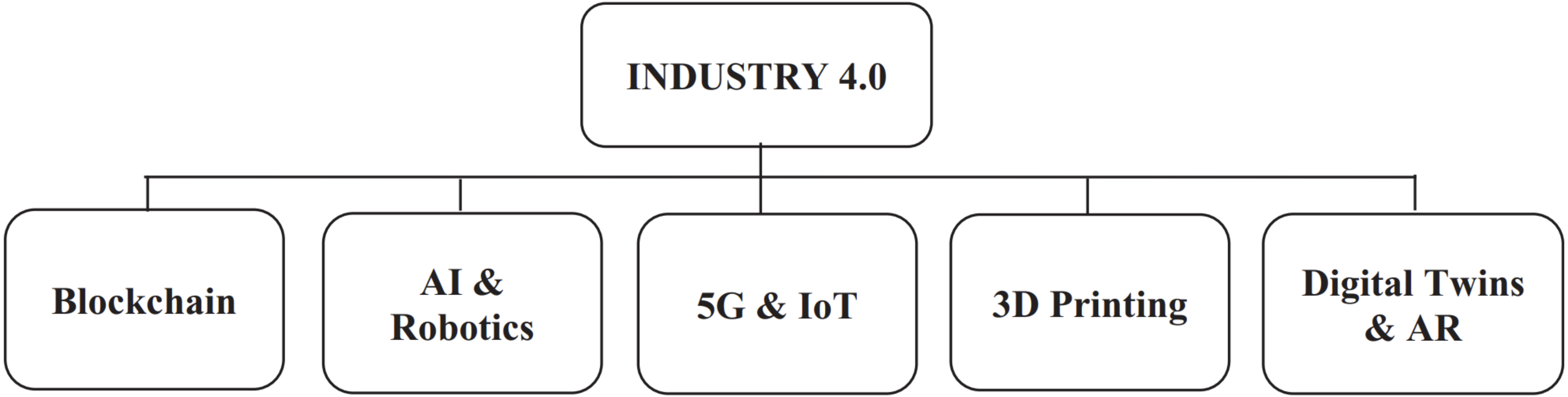
Outline

- Introduction
- Related Literature
- Basic Models
- Values of the government cyber-security penalty schemes
- Extended Models
- Conclusion

Introduction

- □ Industry 4.0 (intelligence; disruptive technologies, Fig. 1 (Choi, Kumar, Yue, Chan 2022))

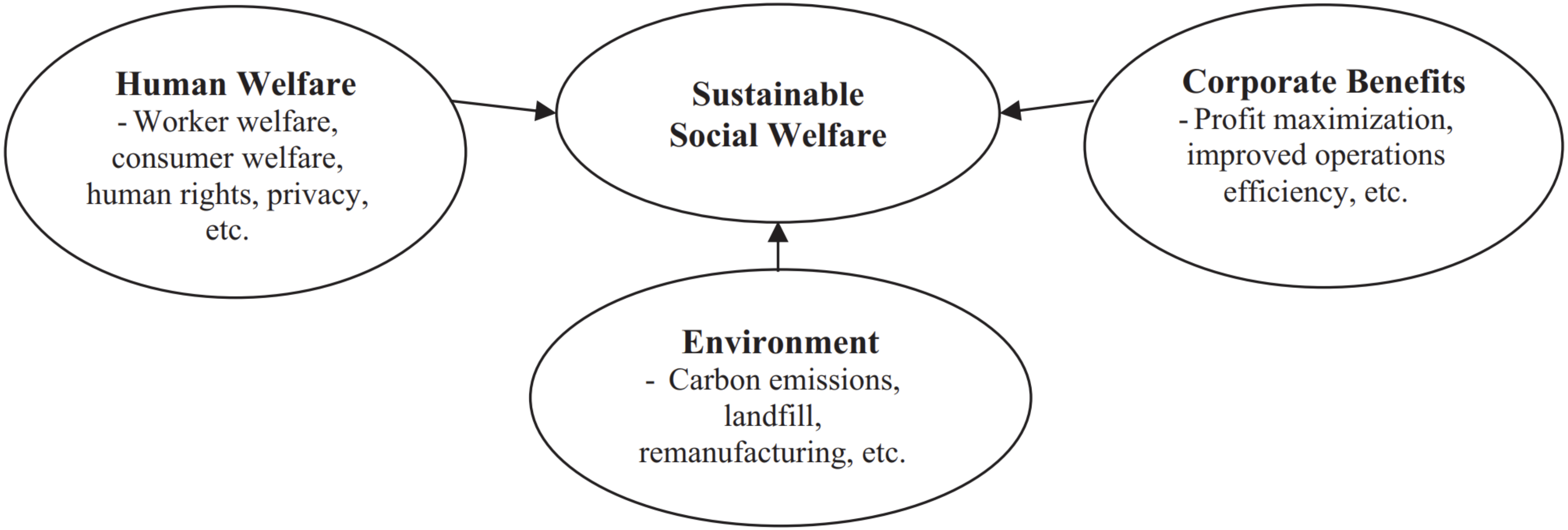
Figure 1 Major Disruptive Technologies in the Industry 4.0 Era



Sustainable social welfare (Choi, Kumar, Yue, Chan 2022)

- Industry 5.0 (Choi et al. 2022)
  - Human concerns are critical and policy makers/governments become crucial.
  - Sustainable social welfare.

Figure 3 The Definition of Sustainable Social Welfare



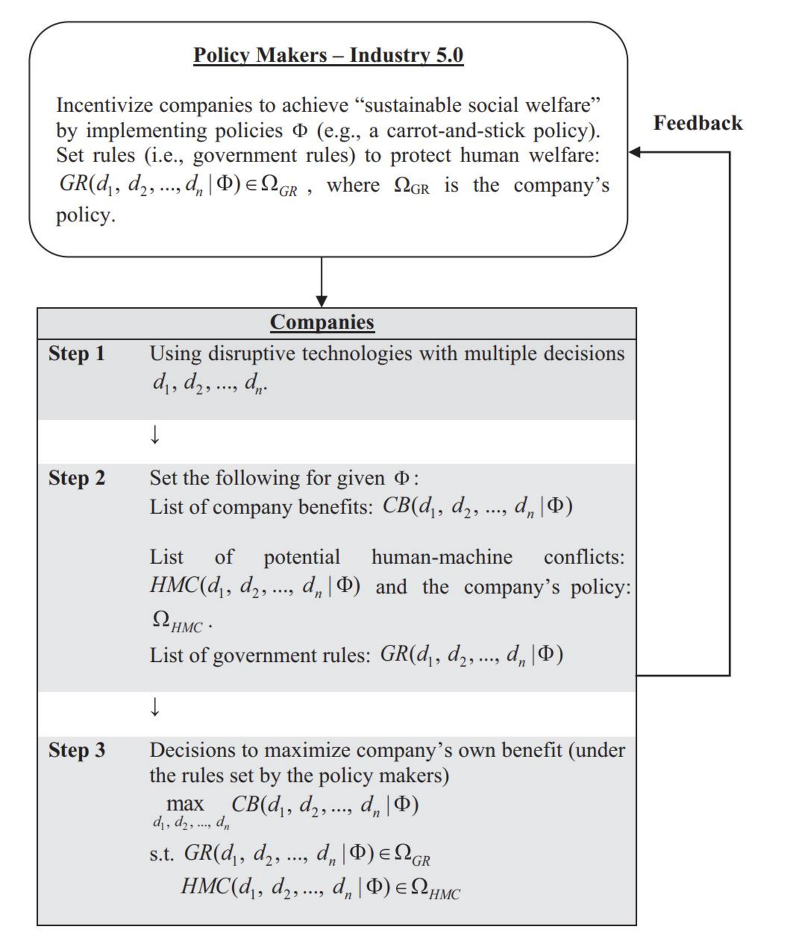
Human Welfare
- Worker welfare, consumer welfare, human rights, privacy, etc.

Sustainable Social Welfare

Corporate Benefits
- Profit maximization, improved operations efficiency, etc.

Environment
- Carbon emissions, landfill, remanufacturing, etc.

Policy makers in Industry 5.0 (Choi, Kumar, Yue, Chan 2022)



Policy Makers – Industry 5.0

Incentivize companies to achieve "sustainable social welfare" by implementing policies Φ (e.g., a carrot-and-stick policy). Set rules (i.e., government rules) to protect human welfare: $GR(d_1, d_2, ..., d_n \mid \Phi) \in \Omega_{GR}$, where Ω_{GR} is the company's policy.

Feedback

Companies

Step 1 Using disruptive technologies with multiple decisions $d_1, d_2, ..., d_n$.

↓

Step 2 Set the following for given Φ :

List of company benefits: $CB(d_1, d_2, ..., d_n \mid \Phi)$

List of potential human-machine conflicts: $HMC(d_1, d_2, ..., d_n \mid \Phi)$ and the company's policy: Ω_{HMC} .

List of government rules: $GR(d_1, d_2, ..., d_n \mid \Phi)$

↓

Step 3 Decisions to maximize company's own benefit (under the rules set by the policy makers)

$$\max_{d_1, d_2, ..., d_n} CB(d_1, d_2, ..., d_n \mid \Phi)$$

$$\text{s.t. } GR(d_1, d_2, ..., d_n \mid \Phi) \in \Omega_{GR}$$

$$HMC(d_1, d_2, ..., d_n \mid \Phi) \in \Omega_{HMC}$$

Introduction | Motivational Case

- **Development of e-commerce.**
  - **Cyber-attacks.**
- **Cyber-security issues are becoming a daily challenge for e-commerce companies (Luo and Choi 2022).**

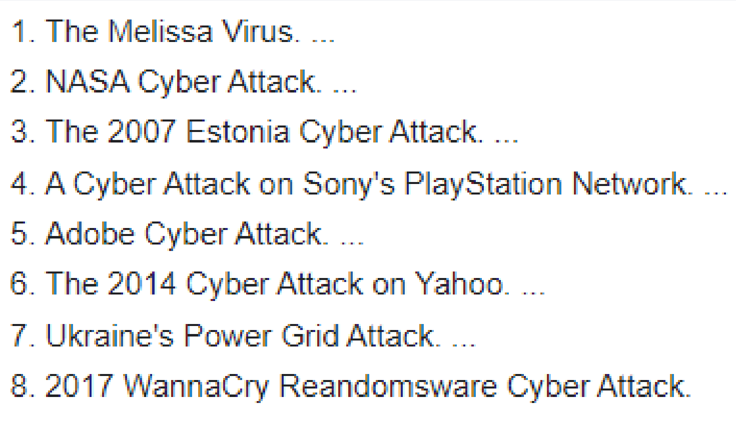
Cyber attacks often have a tremendous impact on companies and individuals (i.e., humans). It is expected that the cost of cyber attacks may reach US$10.5 trillion (= 9.375 trillion pounds) by 2025.

Sources: public news.

Introduction

Motivational Case

□ **Well-reported cyber-attacks:**



1. The Melissa Virus. ...
2. NASA Cyber Attack. ...
3. The 2007 Estonia Cyber Attack. ...
4. A Cyber Attack on Sony's PlayStation Network. ...
5. Adobe Cyber Attack. ...
6. The 2014 Cyber Attack on Yahoo. ...
7. Ukraine's Power Grid Attack. ...
8. 2017 WannaCry Reandomsware Cyber Attack.

Introduction | Motivational Case

- Both e-commerce platforms and governments treat cyber-attacks very seriously, as they can compromise users' privacy and may be disastrous for the companies involved.
  - Credit card details stolen.

A security breach of the giant U.S. retailer Target Corporation in December 2013, for example, exposed the personal data of over 110 million consumers, leading to a nearly 50% drop in profits.

In January 2014, data from 100 million South Korean credit cards were stolen. As a result, more than 2 million South Koreans had their cards blocked or replaced, as they feared that their bank accounts would be emptied.

In 2016, 3 billion Yahoo accounts were hacked, and in 2018, Under Armor reported that its "MyFitnessPal" service had been hacked, affecting 150 million users.

Sony's PlayStation Network was attacked in April 2011, the personal data of 77 million users were leaked and the banking information of tens of thousands of players was compromised.

Introduction

Measures

- □ To prevent consumer information from being stolen, **e-commerce companies** **“should”** implement the right technologies at a non-trivial cost.

Gartner, a leading research firm, predicts that companies’ spending for the information security and risk management market will grow at a “compound annual growth rate” of 8.7% from 2018 through 2023 to reach $188.4 billion.

Introduction

Measures

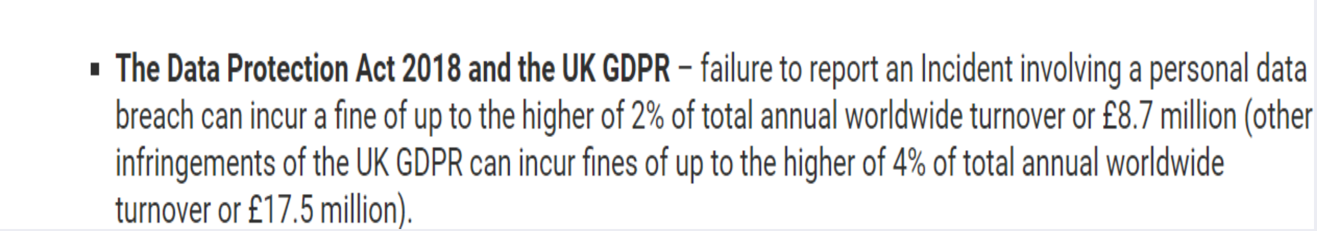
- How about governments?

□ In addition to e-commerce companies' cyber-security measures, **some governments** all around the world have taken actions towards cyber-security related challenges.

Introduction

Table 1.1a. Some examples of cyber-security rules in different places

Rules	Details of penalty
European Union (General Data Protection Regulation)	Very heavy penalty: The maximum fine for non-compliance is €10 million or 2% of "worldwide annual revenue."
New York regulations	No clear penalty imposed for non-compliance
California regulations	Starting from January 1, 2020, "any manufacturer of a device that connects to the internet must equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure." A penalty will be imposed for non-compliance cases.



- **The Data Protection Act 2018 and the UK GDPR** – failure to report an Incident involving a personal data breach can incur a fine of up to the higher of 2% of total annual worldwide turnover or £8.7 million (other infringements of the UK GDPR can incur fines of up to the higher of 4% of total annual worldwide turnover or £17.5 million).

Sources: public news.

Introduction

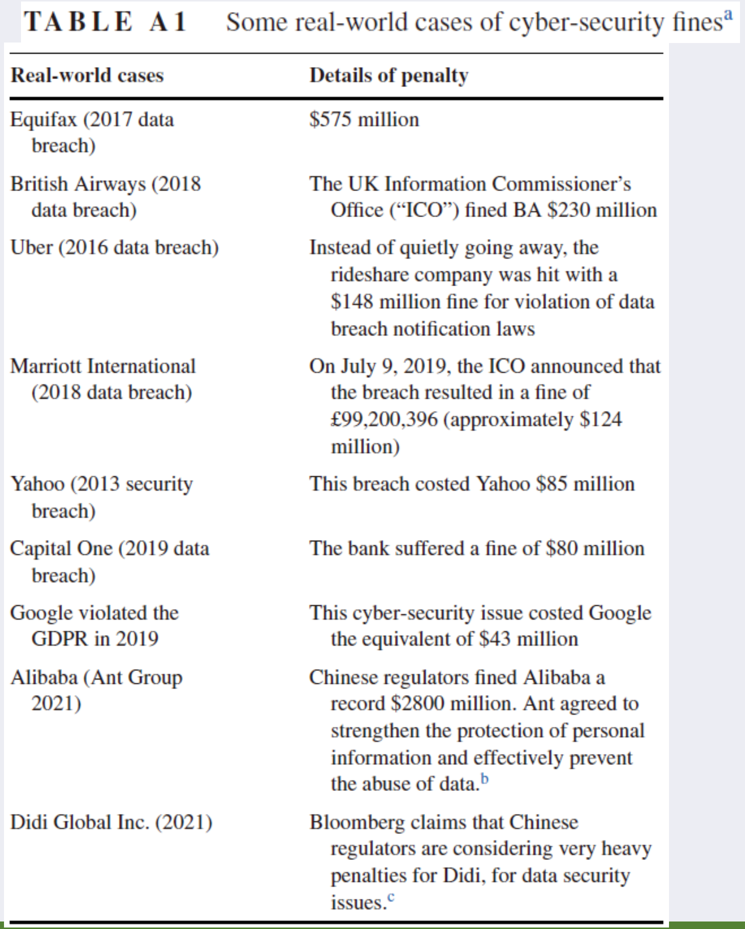


TABLE A1 Some real-world cases of cyber-security fines[a]

Real-world cases	Details of penalty
Equifax (2017 data breach)	$575 million
British Airways (2018 data breach)	The UK Information Commissioner's Office ("ICO") fined BA $230 million
Uber (2016 data breach)	Instead of quietly going away, the rideshare company was hit with a $148 million fine for violation of data breach notification laws
Marriott International (2018 data breach)	On July 9, 2019, the ICO announced that the breach resulted in a fine of £99,200,396 (approximately $124 million)
Yahoo (2013 security breach)	This breach costed Yahoo $85 million
Capital One (2019 data breach)	The bank suffered a fine of $80 million
Google violated the GDPR in 2019	This cyber-security issue costed Google the equivalent of $43 million
Alibaba (Ant Group 2021)	Chinese regulators fined Alibaba a record $2800 million. Ant agreed to strengthen the protection of personal information and effectively prevent the abuse of data.[b]
Didi Global Inc. (2021)	Bloomberg claims that Chinese regulators are considering very heavy penalties for Didi, for data security issues.[c]

ın all the real-world cases that we have found, governments basically always adopt a polarized strategy.

i.e., either do not impose penalty or impose a super heavy penalty, on cyber-security issues. Whether there is a scientific explanation for the existence of this type of polarized strategy deserves deeper investigation.

https://www.statista.com/statistics/1170520/worldwide-data-breach-fines-settlements/ (accessed July 20, 2021)
https://www.ft.com/content/bb251dcc-4bff-4883-9d81-061114fee87f (accessed August 1, 2021)
https://www.bloomberg.com/news/articles/2021-07-22/china-is-said-to-weigh-unprecedented-penalty-for-didi-after-ipo (accessed August 1, 2021)

Sources: public news.

Research Questions

How does the presence of a government cyber-security penalty scheme affect the e-commerce supply chain (and its members), consumers and social welfare?

Polarized strategy: Are there any cases in which having government’s penalty scheme does more harm than good? If it is beneficial to implement the penalty scheme, is it wise for the government to impose a very heavy penalty?

What are the impacts brought by the e-tailer’s deployment of technologies (such as blockchain) on our findings? Are there any other useful supply chain measures to deal with cyber-attacks? How robust are the findings?

Outline

- Introduction
- Related Literature
- Basic Models
- Values of the government cyber-security penalty schemes
- Extended Models
- Conclusion

Related Literature

□ Three streams of OM studies

(i) E-Commerce

Gap and importance: Different from the prior research in e-commerce, we focus on tackling the cyber-security challenge. Unlike other studies, we also examine the government's role in the cyber-security of e-commerce supply chains.

(ii) Cyber-security

Gap and importance: Different from the previous literature, we focus on e-commerce supply chains and analytically study the optimal cyber-security level and the roles played by the government. We also explore the use of blockchain based technologies for enhancing cyber-security.

(iii) The role of government in OM

Gap and importance: We focus on exploring whether governments should play a role (via imposing penalty) on cyber-security, which is motivated by real world observed practices.

Outline

- Introduction
- Related Literature
- Basic Models
- Values of the government cyber-security penalty schemes
- Extended Models
- Conclusion

Basic Models

Model NG

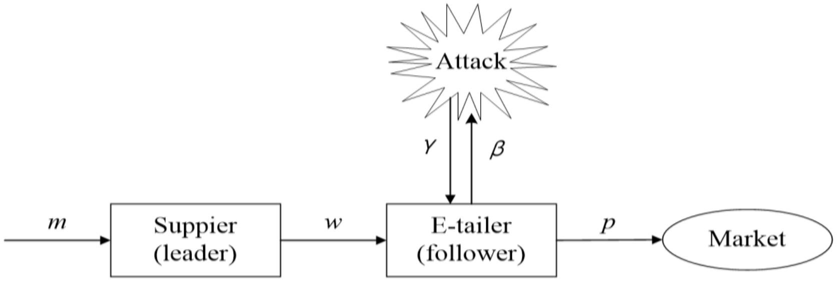


Figure 3. An e-commerce supply chain with cyber-attack (Model NG).

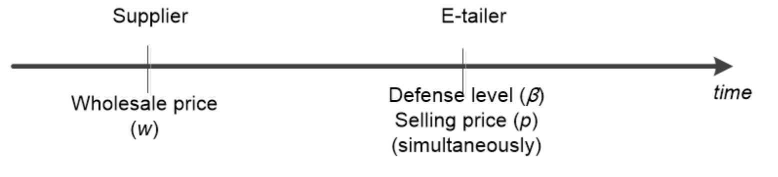


Figure 3.2. Sequence of events for Model NG.

- **We start with a simple "analytically tractable" model.**
- An e-commerce supply chain with a supplier and an e-tailer.
- γ: The likelihood that the e-commerce supply chain faces a cyber-attack.
- β: The rate of success in defending against the cyber-attack.

- **In our model, the supplier determines the wholesale price *w* as the leader and the e-tailer as the follower controls *p* and *β* simultaneously.**

Basic Models- Model NG | General Setups

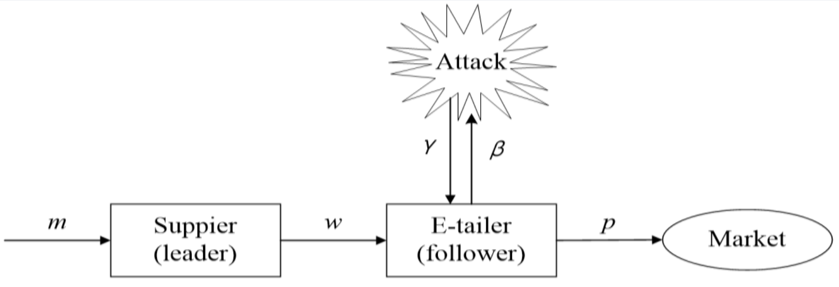


Figure 3. An e-commerce supply chain with cyber-attack (Model NG).

- □ Consumers are heterogenous in their valuation u for the product: u follows a distribution $f(\cdot)$, and $f(u) \sim U\,[0, 1]$.

- □ Demand: $D_{(NG)} = 1 - e + e\beta_{(NG)} - p_{(NG)}$, where $e = a\gamma$.

- □ Profit functions of the supplier (S) and e-tailer (E):

$$\pi_{S(NG)} = \left(w_{(NG)} - m\right)\overbrace{\left(1 - e + e\beta_{(NG)} - p_{(NG)}\right)}^{\text{Demand}}.$$

$$\pi_{E(NG)} = \left(p_{(NG)} - w_{(NG)}\right)\left(1 - e + e\beta_{(NG)} - p_{(NG)}\right) - k\beta_{(NG)}^{2}/2.$$

defense effort cost

Basic Model- Model NG | Equilibrium decisions …

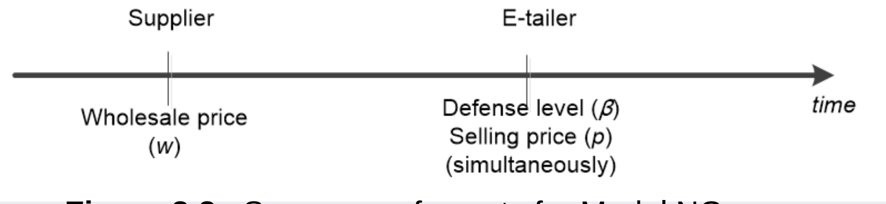


Figure 3.2. Sequence of events for Model NG.

- □ The supplier's profit: $\pi^*_{S(NG)} = 2k\psi$.
- □ The e-tailer's profit: $\pi^*_{E(NG)} = k\psi$.
- □ The consumer surplus: $CS^*_{(NG)} = k\psi(1-B)$.

where $\psi = \frac{(1-e-m)^2}{8(2k-e^2)}$, $A = \frac{k(1-e)}{2k-e^2}$, $B = \frac{k-e^2}{2k-e^2}$,

$\tau = \frac{1-e+m}{2}$, $\varepsilon = 2k - e^2$ and $J = 1 - e - m$.

- ● The selling price: $p^*_{(NG)} = A + \tau B$.
- ● The defense effort set by e-tailer: $\beta^*_{(NG)} = \frac{eJ}{2\varepsilon}$.
- ● The wholesale price set by the supplier: $w^*_{(NG)} = \tau$.

Model G

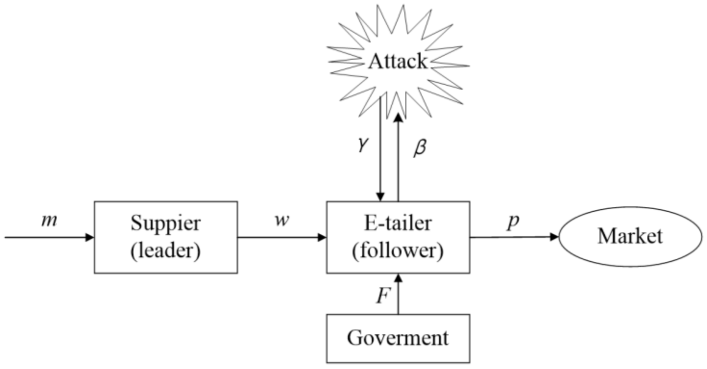


Figure 3. An e-commerce supply chain with government penalty scheme (Model G).

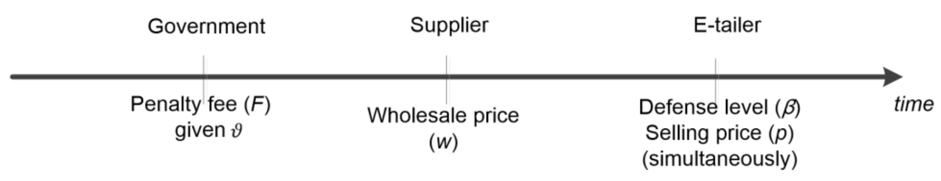


Figure 3.4. Sequence of events for Model G.

- Note that compared to Model NG, the only difference of Model G is that the e-tailer will suffer a penalty F if he fails to defend against the cyber-attack.

- F: The penalty the government imposes on the e-tailer when the e-tailer (E) fails to defend against cyber-attack.

- We define social welfare : $SW^*_{(G)} = \pi^*_{S(G)} + \pi^*_{E(G)} + \vartheta CS^*_{(G)}$, where $\vartheta > 0$ represents the relative importance (weight) of consumer surplus in the social welfare. **[P.S.: INDUSTRY 5.0 (Choi et al. 2022)]**

- In most prior literature, this value is set to be 1 but as we will see later on, ϑ is in fact critical for our analysis and hence we explicitly define it here.

Basic Models

General Setups for Model G

Model G

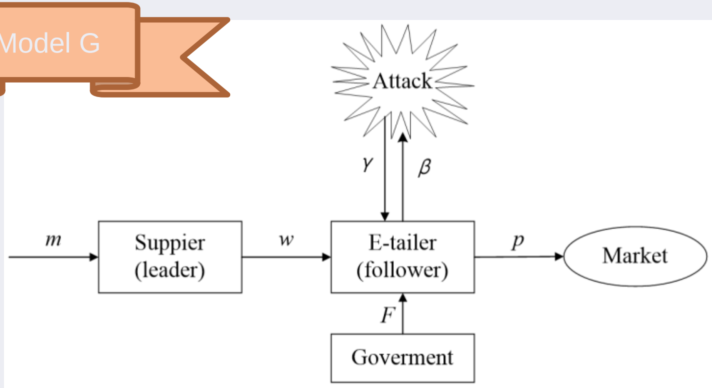


Figure 3. An e-commerce supply chain with government penalty scheme (Model G

- □ Demand: $D_{(G)} = 1 - e + e\beta_{(G)} - p_{(G)}$.

- □ Profit functions of the supplier (S) and e-tailer (E):

$$\pi_{S(G)} = (w_{(G)} - m)(1 - e + \overbrace{e\beta_{(G)} - p_{(G)})}^{\text{Demand}}.$$

$$\pi_{E(G)} = (p_{(G)} - w_{(G)})D_{(G)}\left(1 - \gamma(1 - \beta_{(G)})\right) + [(p_{(G)} - w_{(G)})D_{(G)} - F]\gamma(1 - \beta_{(G)}) - \underbrace{\frac{k\,\beta_{(G)}^2}{2}}_{\text{The penalty fee}}.$$

Basic Models- Model G

Equilibrium decisions…

- $w^{*}_{(G)} = \frac{k(1-e+m)+eF\gamma}{2k} = \tau + \boldsymbol{C} \cdot \boldsymbol{F},$
- $p^{*}_{(G)} = A + \tau B + (\boldsymbol{2} - \boldsymbol{B})\boldsymbol{C} \cdot \boldsymbol{F},$
- $\beta^{*}_{(G)} = \frac{eJ}{2\varepsilon} + \frac{(\boldsymbol{3-2B})\boldsymbol{C \cdot F}}{\boldsymbol{e}}$, where $C = \frac{e\gamma}{2k}$.

□ The supplier’s profit: $\pi^{*}_{S(G)} = \frac{(k(1-e-m)+eF\gamma)^2}{4((2k-e^2)k} = \frac{2d\varepsilon}{k}$.

□ The e-tailer’s profit: $\pi^{*}_{E(G)} = \frac{k^2(1-e-m)^2-2Fk\gamma(8k-e(1+3e-m))+F^2\gamma^2(8k-3e^2)}{8(2k-e^2)k} = M_1$.

□ The consumer surplus: $CS^{*}_{(G)} = d$, where $d = \frac{(k(1-e-m)+eF\gamma)^2}{8(2k-e^2)^2}$.

□ The social welfare: $SW^{*}_{(G)} = \frac{2d\varepsilon}{k} + M_1 + \vartheta d$.

Note that we only discuss the case when e-tailer’s profit is positive and the effort level is less than the upper bound. The penalty fee should be less than $\overline{F} \equiv \frac{k(4k-e(1+e-m))}{(4k-e^2)\gamma}$ and $4k > e(1 + e - m)$ under Model G.

Basic Models- Model G

Equilibrium decisions

- □ **Sensitivity analyses for Models G and NG**

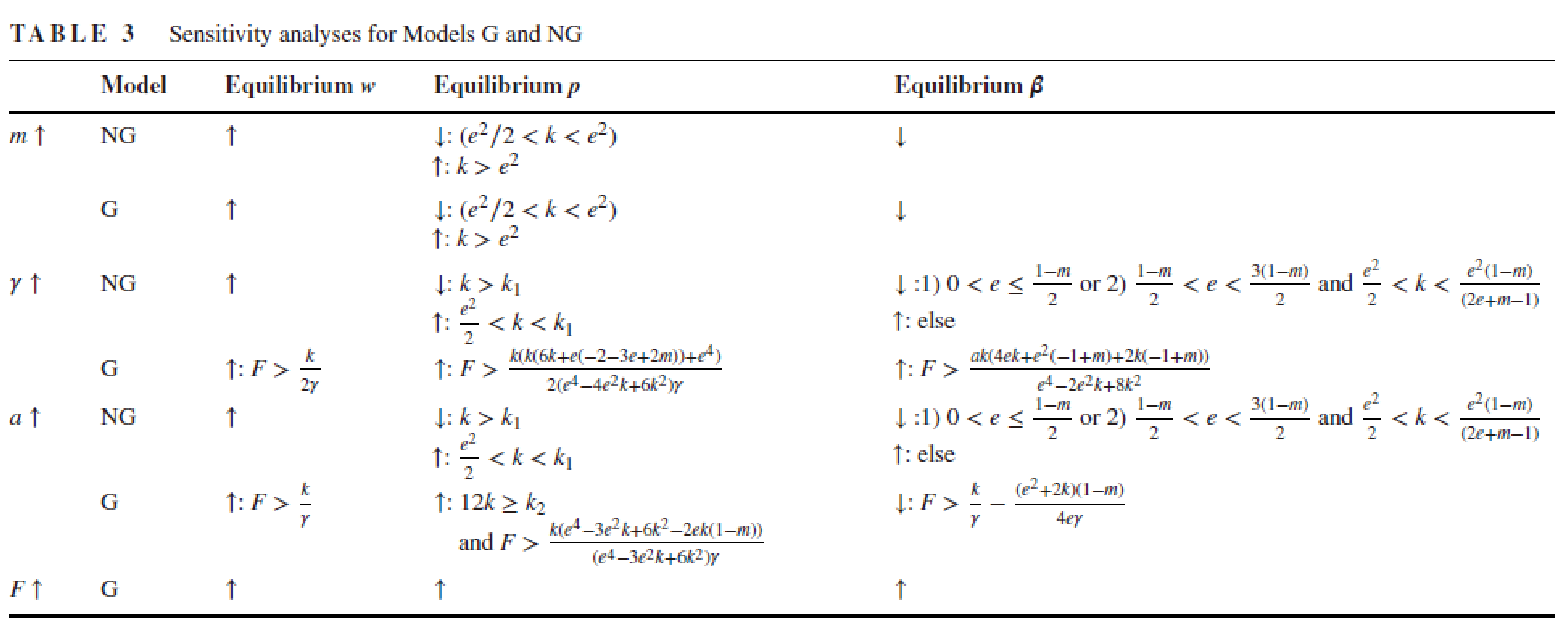


TABLE 3 Sensitivity analyses for Models G and NG

	Model	Equilibrium w	Equilibrium p	Equilibrium β
$m \uparrow$	NG	$\uparrow$	$\downarrow$: $(e^2/2 < k < e^2)$ $\uparrow$: $k > e^2$	$\downarrow$
	G	$\uparrow$	$\downarrow$: $(e^2/2 < k < e^2)$ $\uparrow$: $k > e^2$	$\downarrow$
$\gamma \uparrow$	NG	$\uparrow$	$\downarrow$: $k > k_1$ $\uparrow$: $\frac{e^2}{2} < k < k_1$	$\downarrow$:1) $0 < e \leq \frac{1-m}{2}$ or 2) $\frac{1-m}{2} < e < \frac{3(1-m)}{2}$ and $\frac{e^2}{2} < k < \frac{e^2(1-m)}{(2e+m-1)}$ $\uparrow$: else
	G	$\uparrow$: $F > \frac{k}{2\gamma}$	$\uparrow$: $F > \frac{k(k(6k+e(-2-3e+2m))+e^4)}{2(e^4-4e^2k+6k^2)\gamma}$	$\uparrow$: $F > \frac{ak(4ek+e^2(-1+m)+2k(-1+m))}{e^4-2e^2k+8k^2}$
$a \uparrow$	NG	$\uparrow$	$\downarrow$: $k > k_1$ $\uparrow$: $\frac{e^2}{2} < k < k_1$	$\downarrow$:1) $0 < e \leq \frac{1-m}{2}$ or 2) $\frac{1-m}{2} < e < \frac{3(1-m)}{2}$ and $\frac{e^2}{2} < k < \frac{e^2(1-m)}{(2e+m-1)}$ $\uparrow$: else
	G	$\uparrow$: $F > \frac{k}{\gamma}$	$\uparrow$: $12k \geq k_2$ and $F > \frac{k(e^4-3e^2k+6k^2-2ek(1-m))}{(e^4-3e^2k+6k^2)\gamma}$	$\downarrow$: $F > \frac{k}{\gamma} - \frac{(e^2+2k)(1-m)}{4e\gamma}$
$F \uparrow$	G	$\uparrow$	$\uparrow$	$\uparrow$

Outline

- Introduction
- Related Literature
- Basic Models
- Values of the government cyber-security penalty schemes
- Extended Models
- Conclusion

Values of Government Cyber-Security Penalty Schemes

Proposition 4.1. . *For given* $a,\ m,\ k$ *and* γ: $w^*_{(G)} > w^*_{(NG)}; p^*_{(G)} > p^*_{(NG)};\ \beta^*_{(G)} > \beta^*_{(NG)}$; $\pi_S{}^*{}_{(G)} > \pi_S{}^*{}_{(NG)};\ CS^*_{(G)} > CS^*_{(NG)}$.

Findings:

In the presence of government cyber-security penalty schemes: “the wholesale price, the selling price, and the defense effort” all increase, as do the supplier’s profit and consumer surplus.

Values of Government Cyber-Security Penalty Schemes

- Comparisons between Model NG and Model G:

The values of government cyber-security penalty schemes (VGCPS) for the supplier, the e-tailer, consumers, and social welfare:

$$VGCPS_{(S)} = \pi^*_{S(G)} - \pi^*_{S(NG)}.$$

$$VGCPS_{(E)} = \pi^*_{E(G)} - \pi^*_{E(NG)}.$$

$$VGCPS_{(CS)} = CS^*_{(G)} - CS^*_{(NG)}.$$

$$VGCPS_{(SW)} = SW^*_{(G)} - SW^*_{(NG)}.$$

- $VGCPS_{(S)}$ and $VGCPS_{(CS)}$ are always positive whereas $VGCPS_{(E)}$ is negative.
- For $VGCPS_{(SW)}$, we find that it is negative when $\vartheta = 1$.

Values of Government Cyber-Security Penalty Schemes

- How various parameters affect $VGCPS_{(SW)}$ with different ϑ:

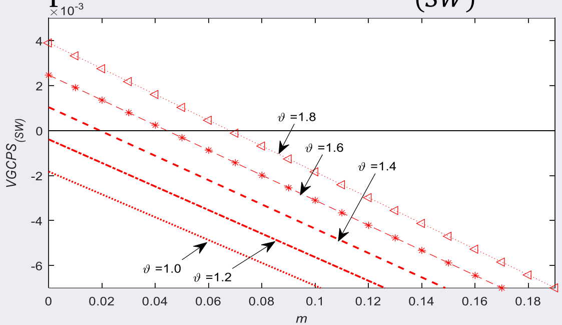


Figure 4.1. How m affects $VGCPS_{(SW)}$

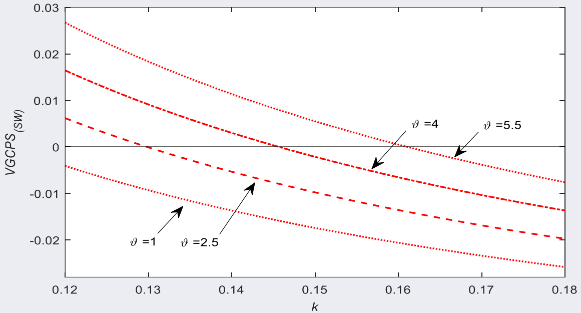
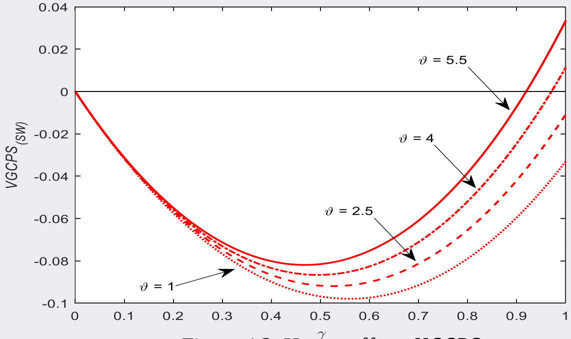


Figure 4.2. How k affects $VGCPS_{(SW)}$



. Figure 4.3. How γ affects $VGCPS_{(SW)}$.

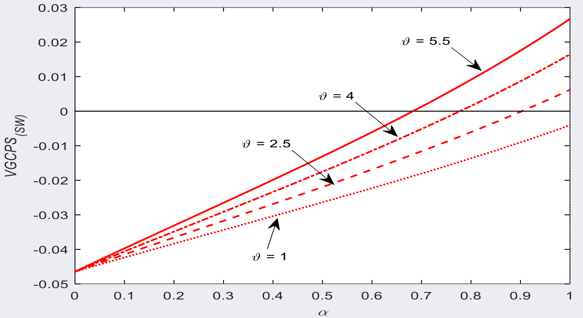


Figure 4.4. How α affects $VGCPS_{(SW)}$.

- If the government puts a higher emphasis on *CS*, then $VGCPS_{(SW)}$ will become positive.

Values of Government Cyber-Security Penalty Schemes

- To be specific, $VGCPS_{(SW)} \geq 0$ if and only if $\vartheta \geq T \equiv \frac{(2k-e^2)(2k(8k-e(3+e-3m))-F(8k-e^2)\gamma)}{ek(2k(1-e-m)+eF\gamma)}$.
- Under Model G, F is bounded above by $\overline{F} \equiv \frac{k(4k-e(1+e-m))}{(4k-e^2)\gamma}$ (or else the e-tailer will quit the market).
- Notation:
  - $\lim_{F \to 0} T = \overline{T} \equiv \frac{(2k-e^2)(8k-e(3+e-3m))}{ek(1-e-m)}$.
  - $\underline{T} \equiv \frac{(2k-e^2)(e^4-12e^2k+32k^2+5e^3(1-m)-16ek(1-m))}{ek(e^3-4ek-3e^2(1-m)+8k(1-m))}$. $(\mathrm{P.S.:}\ F = \overline{F})$

Values of Government Cyber-Security Penalty Schemes

Theorem 4.1.

(a) It is wise for the government to impose the penalty scheme if and only if $\vartheta > T \equiv \frac{(2k-e^2)(2k(8k-e(3+e-3m))-F(8k-e^2)\gamma)}{ek(2k(1-e-m)+eF\gamma)}$ *and the optimal F =* $\overline{F}$ *(i.e., the upper bound). Otherwise, if* $\vartheta \le T$*, then the government should not impose the penalty.*

(b) Under Model G (in which the government imposes a penalty fee less than $\overline{F}$*), then when the government's penalty fee increases: (i) Both the supplier and consumer are always benefited from the scheme. However, the e-tailer's profit is hurt. (ii) If the government puts a sufficiently high emphasis on CS (i.e.,* $\vartheta\overline{T}$*), social welfare increases.*

- As a remark, when $\underline{T} < \vartheta < \overline{T}$, Model G yields a higher social welfare than Model NG if the government imposes a penalty fee between $[\ddot{F}, \overline{F}]$,where $\ddot{F} = arg_F(T = \vartheta)$; if $\vartheta < \underline{T}$, the penalty scheme should not be implemented.

Values of Government Cyber-Security Penalty Schemes

Theorem 4.1.

(a) It is wise for the government to impose the penalty scheme if and only if $\vartheta > T \equiv \frac{(2k-e^2)(2k(8k-e(3+e-3m))-F(8k-e^2)\gamma)}{ek(2k(1-e-m)+eF\gamma)}$ *and the optimal F =* $\overline{F}$ *(i.e., the upper bound). Otherwise, if* $\vartheta \leq T$, *then the government should not impose the penalty.*

(b) Under Model G (in which the government imposes a penalty fee less than $\overline{F}$*), then when the government's penalty fee increases: (i) Both the supplier and consumer are always benefited from the scheme. However, the e-tailer's profit is hurt. (ii) If the government puts a sufficiently high emphasis on CS (i.e.,* $\vartheta\overline{T}$*), social welfare increases.*

- It is impossible to achieve the "all-win situation" under Model G (compared to Model NG) : the e-tailer is always worse off.
- For the governments which treasure consumer welfare more, it is appropriate to implement penalty schemes.

Values of Government Cyber-Security Penalty Schemes

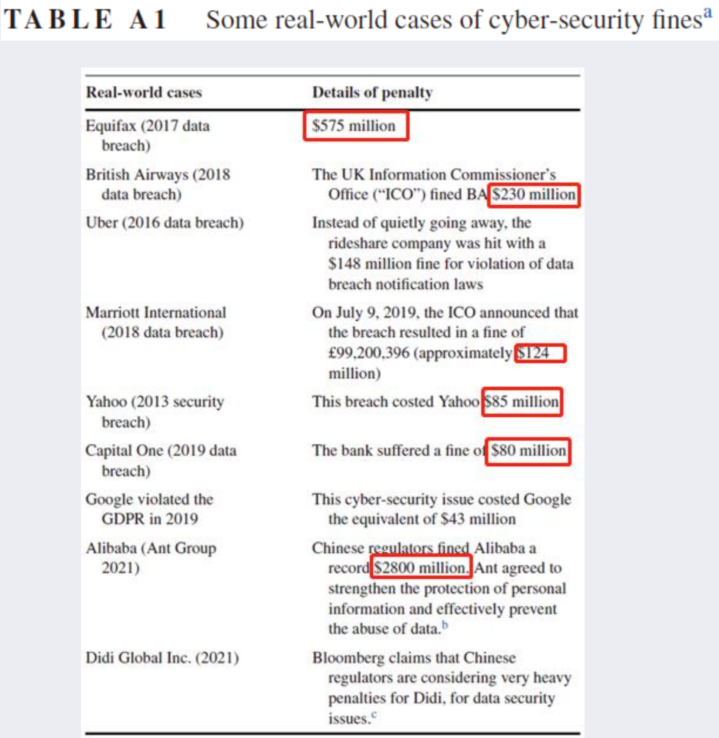


TABLE A1 Some real-world cases of cyber-security fines[a]

Real-world cases	Details of penalty
Equifax (2017 data breach)	$575 million
British Airways (2018 data breach)	The UK Information Commissioner's Office ("ICO") fined BA $230 million
Uber (2016 data breach)	Instead of quietly going away, the rideshare company was hit with a $148 million fine for violation of data breach notification laws
Marriott International (2018 data breach)	On July 9, 2019, the ICO announced that the breach resulted in a fine of £99,200,396 (approximately $124 million)
Yahoo (2013 security breach)	This breach costed Yahoo $85 million
Capital One (2019 data breach)	The bank suffered a fine of $80 million
Google violated the GDPR in 2019	This cyber-security issue costed Google the equivalent of $43 million
Alibaba (Ant Group 2021)	Chinese regulators fined Alibaba a record $2800 million. Ant agreed to strengthen the protection of personal information and effectively prevent the abuse of data.[b]
Didi Global Inc. (2021)	Bloomberg claims that Chinese regulators are considering very heavy penalties for Didi, for data security issues.[c]

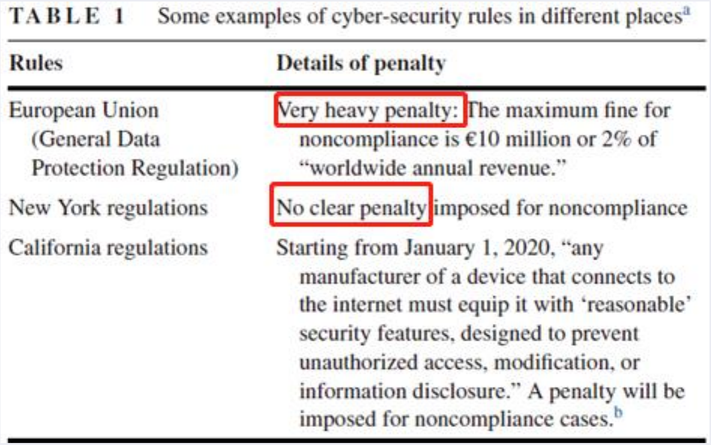


TABLE 1 Some examples of cyber-security rules in different places[a]

Rules	Details of penalty
European Union (General Data Protection Regulation)	Very heavy penalty: The maximum fine for noncompliance is €10 million or 2% of "worldwide annual revenue."
New York regulations	No clear penalty imposed for noncompliance
California regulations	Starting from January 1, 2020, "any manufacturer of a device that connects to the internet must equip it with 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure." A penalty will be imposed for noncompliance cases.[b]

- Theorem 4.1 may hence explain why some governments (such as European Union) have implemented the penalty scheme but some (e.g., New York) do not.

- The polarized policy is optimal.

Sources: public news.

Outline

- Introduction
- Related Literature
- Basic Models
- Values of the government cyber-security penalty schemes
- Extended Models
- Conclusion

Extended Models

Extensions

- □ **Using Blockchain-Based Systems Security Enhancing Technologies**

- □ **Other Extensions**

  - ◆ **Alliance**：The supplier and e-tailer form a strategic alliance and be vertically integrated.
  - ◆ **Competition**： A stylized supply chain consisting of two competing e-tailers (called e-tailers 1 and 2) selling two substitutable products: (a) without government's penalty; (b) with government's penalty.
  - ◆ **Defense-level dependent penalty**：The government's penalty F is a function of β.

Extended Models

Extensions

□ **Using Blockchain-Based Systems Security Enhancing Technologies**

- □ **IBM Blockchain, Alibaba Cloud.**
- □ **Extension (Model NT)**：The e-tailer adopts technologies to defend against cyber-attack without government penalty.

□ Demand: $D_{(NT)} = \int_{p+a\alpha-b}^{1} f(u)\,du = 1 + b - e + e\,\beta_{(NT)} - p_{(NT)},$

□ The profit functions of supplier (S) and e-tailer (E):

$$\pi_{E(NT)} = \left(p_{(NT)} - w_{(NT)} - c\right)D_{(NT)} - K^{IT}\left(\beta_{(NT)}\right) - \; T^{IT}$$

$$\pi_{S(NT)} = \left(w_{(NT)} - m\right)D_{(NT)},$$

- b > 0 is the benefit brought to consumers with the use of technologies (e.g., blockchain).
- where $K^{IT}\left(\beta_{(NT)}\right) = k^{IT}\beta_{(NT)}^{2}/2$ and $k^{IT} < k$;
- $c > 0$ is the per unit technologies operations cost;
- $T^{IT} > 0$ is the fixed technologies cost.

Extended Models

□ **Using Blockchain-Based Systems Security Enhancing Technologies**

□ **Extension (Model NT)** : The e-tailer adopts technologies to defend against cyber-attack without government penalty.

Define: technology benefit-to-cost ratio: $BCR = b/c$.

Theorem 5.1. *Under the case without government penalty, if $BCR \geq 1$, the e-tailer's use of technologies such as blockchain (i.e., comparing between Model NG and Model NT) will yield the following:*

(a) The cyber-security level is higher.

(b) Both the supplier and consumers are benefited.

(c) When T^{IT} is sufficiently small, the e-tailer is benefited and social welfare is improved. When T^{IT} is moderate, social welfare is improved but the e-tailer suffers a loss. When T^{IT} is sufficiently big, the e-tailer suffers a loss and social welfare drops.

- $b > 0$ is the benefit brought to consumers with the use of technologies (e.g., blockchain).
- $c > 0$ is the per unit technologies operations cost;

- We find that the main difference between Model NG and Model NT is related to factors *including BCR (i.e., b and c)* and T^{IT}

The adoption of blockchain technologies can increase the cybersecurity level and bring benefit to all members when the benefit brought to consumers with the use of technologies (b) is greater or slightly less than the per unit technology operations cost (c) and the fixed technology cost (T^{IT}) is not very high. **[In fact intuitive]**

Extended Models

Extensions

- □ **Using Blockchain-Based Systems Security Enhancing Technologies**
  - □ **Extension (Model GT)**：The e-tailer makes use of technologies with government penalty.

Proposition 5.1. *If it is beneficial for the government to impose the penalty, comparing between Model G and Model GT: When,* $BCR > 1$, *then the optimal penalty is smaller after adopting technologies (such as blockchain). Otherwise, if the* $BCR < 1$ *(BCR = 1), then the optimal penalty is larger (unchanged) after technology adoption.*

Extended Models

□ **Using Blockchain-Based Systems Security Enhancing Technologies**

◆ **Model NT**：The e-tailer adopts technologies to defend against cyber-attack without government penalty.

◆ **Model GT**：The e-tailer makes use of technologies with government penalty.

□ **Other Extensions**

◆ **Alliance**：The supplier and e-tailer form a strategic alliance and become vertically integrated.

◆ **Competition**： A stylized supply chain consisting of two competing e-tailers (called e-tailers 1 and 2) selling two substitutable products. (a) without government's penalty; (b) with government's penalty.

◆ **Defense-level dependent penalty**：the government's penalty F is a function of β.

Extended Models

Extensions

□ Other Extensions

- **Alliance**：The supplier and e-tailer form a strategic alliance and be integrated.

Findings: By forming the supply chain alliance, the cyber security level, the profit of the whole supply chain, consumer surplus, and social welfare will all be better! **Forming an alliance, as an all-win strategy, is a very effective way for improving cybersecurity level.** This is consistent with the observed industrial practices that major e-tailers like Amazon.com and JD.com all have formed strategic alliances with many of their suppliers.

Extended Models

- □ **Other Extensions**
  - ◆ **Competition**
  - ◆ **Defense-level dependent penalty**： the government's penalty F is a function of β.

The results derived under the basic models stay robust.

Outline

- Introduction
- Related Literature
- Basic Models
- Values of the government cyber-security penalty schemes
- Extended Models
- Conclusion

Conclusion

Major Findings and Managerial Insights

□ **The government’s cyber-security penalty scheme:**

- The government’s penalty scheme will always benefit the supplier and consumers but hurt the e-tailer.
- We have analytically proven (with the bounds derived) that when the government’s emphasis on consumer surplus is sufficiently high, implementing the penalty scheme is beneficial to social welfare.

□ **The optimal penalty scheme:**

- Polarized.

Conclusion

Major Findings and Managerial Insights

□ **Using systems security enhancing technologies (such as blockchain):**

- It is interesting to note that when it is beneficial to have the government penalty scheme, how the presence of blockchain affects the optimal penalty depends on the technology benefit-to-cost ratio (*BCR*) (as shown in Proposition 5.1)

Proposition 5.1. *If it is beneficial for the government to impose the penalty, comparing between Model G and Model GT: When, $BCR > 1$, then the optimal penalty is smaller after adopting technologies (such as blockchain). Otherwise, if the $BCR < 1$ (BCR = 1), then the optimal penalty is larger (unchanged) after technology adoption.*

Conclusion

Major Findings and Managerial Insights

□ **What if it is not beneficial to have the cyber-security penalty scheme?**

- Establishing an alliance strategy is an essential measure to help achieve an all-win situation and governments should not ignore its importance.
- This finding also supports the common observations that e-commerce supply chain members love to establish alliances (as evidenced by the cases of Amazon.com and JD.com).

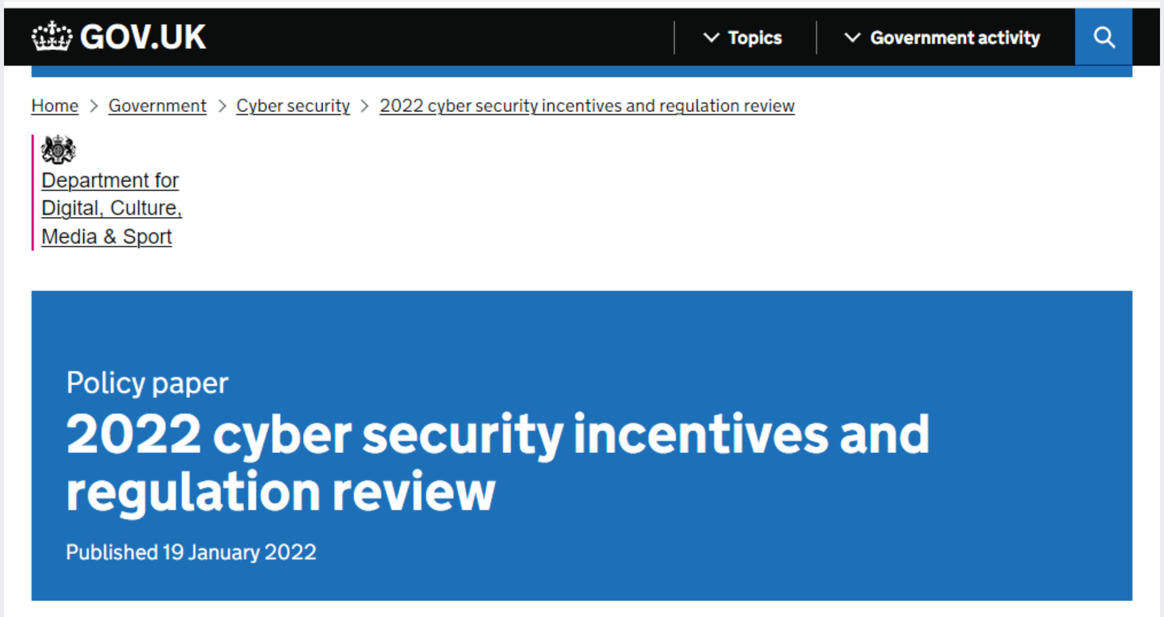
□ **Robustness of findings:**

- Shown via various extensions.

Conclusion

□ Limitations and Future directions

- We consider the information symmetry case in this paper and postpone the case with asymmetric information to future research.
- Other issues:
  - Setting standards?



Home > Government > Cyber security > 2022 cyber security incentives and regulation review

Department for Digital, Culture, Media & Sport

Policy paper

2022 cyber security incentives and regulation review

Published 19 January 2022

References

Babich, V., G. Hilary. 2019. Distributed ledgers and operations: What operations management researchers should know about blockchain technology. Manufacturing & Service Operations Management 22(2), 223-240. [Blockchain discussion]

Cheung, K. F., M.G. Bell. 2019. Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research 291(2), 471-481. [Cyber-security]

Choi, T.M., S. Kumar, X. Yue, H.L. Chan. Disruptive technologies and operations management in the Industry 4.0 era and beyond. Production and Operations Management, 31(1), 9-31, 2022.

Choi, T.M., S.W. Wallace, Y. Wang. 2018. Big data analytics in operations management. Production and Operations Management 27(10), 1868-1883.

Liu, W., J. Wang, F. Jia, T.M. Choi. Blockchain announcements and stock value: A technology management perspective. International Journal of Operations and Production Management, 42(5), 713-724, 2022. [Empirical blockchain]

Luo, S., T.M. Choi. E-commerce supply chains with considerations of cyber-security: Should governments play a role? Production and Operations Management, 31 (5), 2107-2126, 2022.

References

Olsen, T.L., B. Tomlin. 2020. Industry 4.0: Opportunities and challenges for operations management. Manufacturing & Service Operations Management 22(1), 113-122.

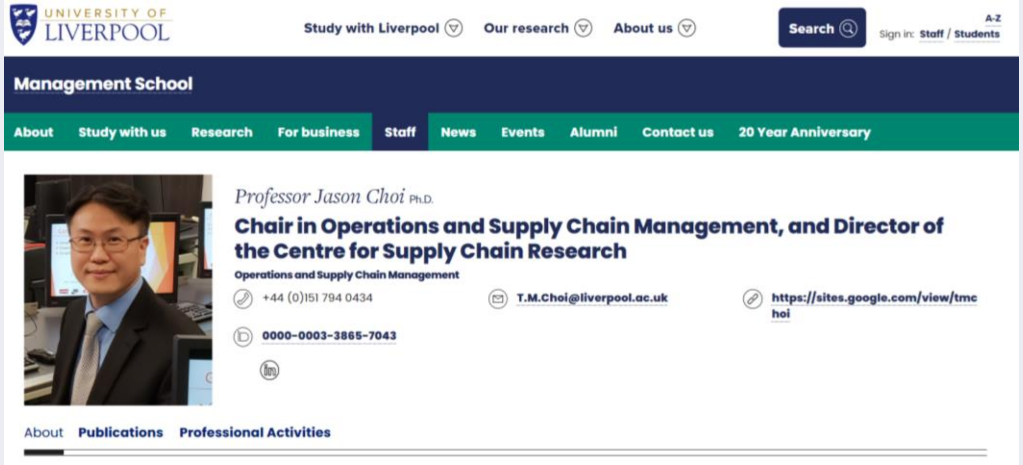
Pun, H., J.M. Swaminathan, P. Hou. 2021. Blockchain adoption for combating deceptive counterfeits. Production and Operations Management 30(4), 864-882. [Analytical blockchain]

Shen, B., C. Dong, S. Minner. 2022. Combating copycats in the supply chain with permissioned blockchain technology. Production and Operations Management, 31(1), 138-154. [Analytical blockchain]

Sheu, J.B., T.M. Choi. 2022. Can we work more safely and healthily with robot partners? A human-friendly robot-human coordinated order fulfillment scheme. Production and Operations Management, accepted. [Industry 5.0]

Simon, J., A. Omar. 2020. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. European Journal of Operational Research 282(1), 161-171.

Professor Tsan-Ming CHOI (Jason)
Chair in Operations and Supply Chain Management
Director of the Centre for Supply Chain Research
University of Liverpool Management School, United Kingdom
Email: t.m.choi@liverpool.ac.uk



Professor Jason Choi Ph.D.

Chair in Operations and Supply Chain Management, and Director of the Centre for Supply Chain Research

Operations and Supply Chain Management

+44 (0)151 794 0434

T.M.Choi@liverpool.ac.uk

https://sites.google.com/view/tmchoi

0000-0003-3865-7043

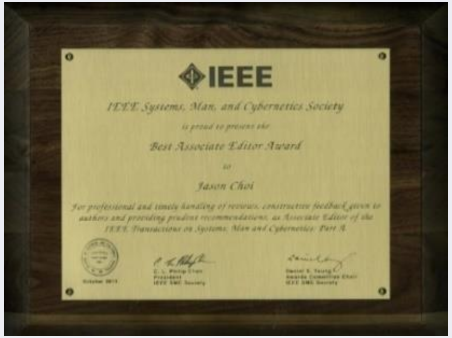
Services:

Co-Editor-in-Chief: ***Transportation Research Part E***
SE: *Production and Operations Management, DSS*
DE: *IEEE Transactions of Engineering Management*
AE: *Decision Sciences, IEEE-T-SMC-S*

RGC(HK) Panel member

Chair: Blockchain for SCM (SiG, IEEE-TEMS)

IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT
IEEE
A PUBLICATION ON THE IEEE TECHNOLOGY AND ENGINEERING MANAGEMENT SOCIETY
FEBRUARY 2021
VOLUME 68
NUMBER 1
IEEMA4
IEEE TEMS



IEEE

IEEE Systems, Man, and Cybernetics Society

is proud to present the

Best Associate Editor Award

to

Jason Choi

For professional and timely handling of reviews, constructive feedback given to authors and providing prudent recommendations, as Associate Editor of the IEEE Transactions on Systems, Man and Cybernetics: Part A.

October 2013

C. L. Philip Chen
President
IEEE SMC Society

Daniel S. Yeung
Awards Committee Chair
IEEE SMC Society

Thank you!

IIC2022

ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

Assoc. Prof. John Luke Gallup

Economics Dept., Portland State
University, Portland, Oregon, USA

Dr. Gallup does research on the Vietnamese Economy, Economic Growth, Automation, Health, and Economic Geography. He received his PhD in Economics and MA in Demography from U.C. Berkeley (US) and his BA in Economics and Politics from Swarthmore College (US). He previously taught at Harvard University, as a Fulbright Scholar at the University of Commerce (Vietnam), and as a visiting scholar at the Toulouse School of Economics (France). Dr. Gallup's recent research assesses the impact of early child development on economic growth, the theory of added-value plots, the economic impact of tropical disease, and the effect of economic development on income distribution. He has consulted for the World Bank, UNDP, EU, ADB, ILO, USAID, multiple Vietnamese Ministries, and the Government of Bolivia. He has won awards for teaching graduate and undergraduate Development Economics and Econometrics courses. Dr. Gallup has 9,041 citations in Google Scholar and has served as a referee for 33 academic journals. He has conducted economic research in Vietnam since 1993 and speaks Vietnamese.

IIC2022
ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

EIU

CỤC CÔNG TÁC PHÍA NAM

The 2nd International Conference on Advanced Technology & Sustainable Development (ICATSD 2022)

DEVELOPMENT STRATEGY AND INTELLECTUAL INFRASTRUCTURE

JOHN LUKE GALLUP

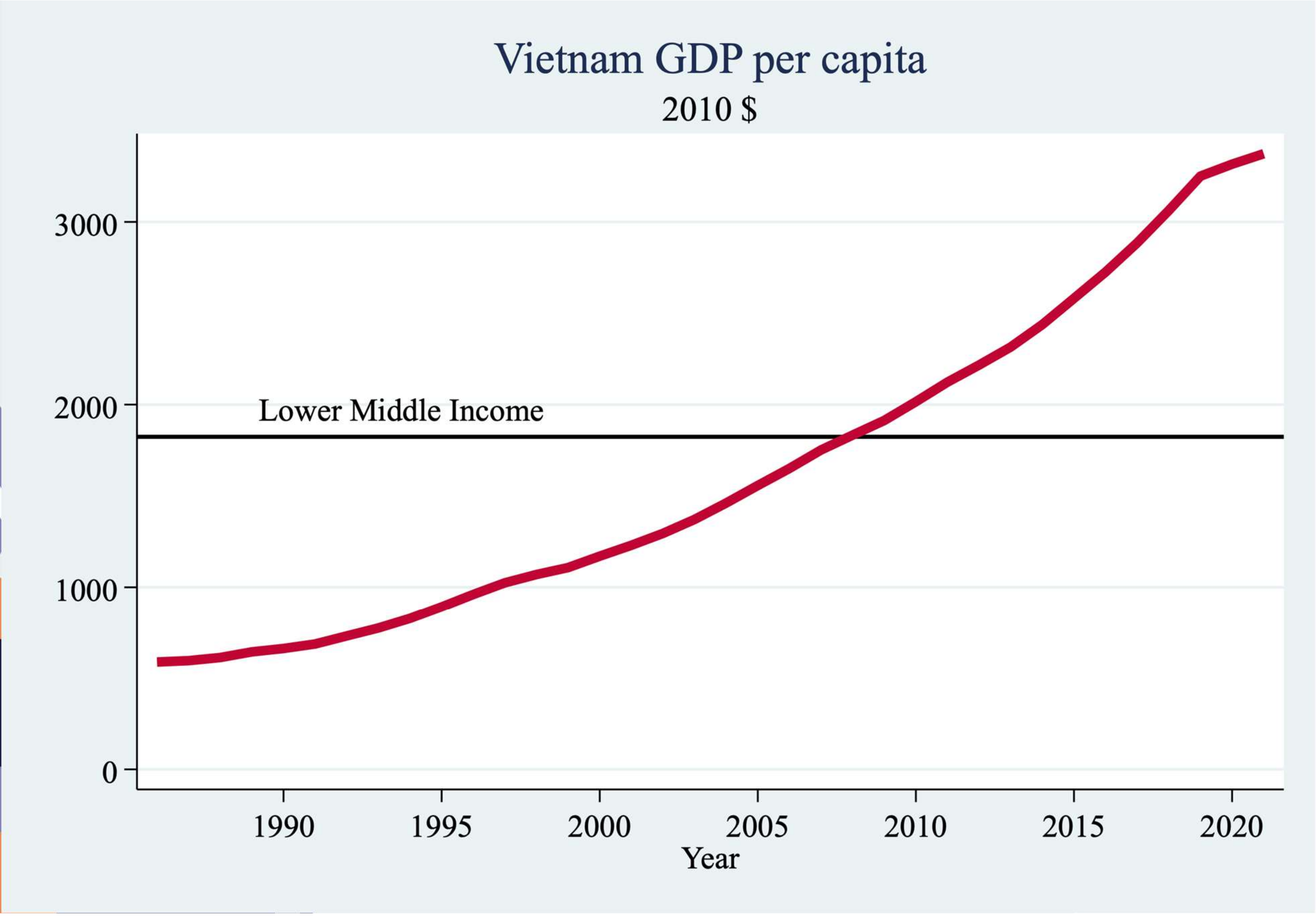
Portland State University, USA

Dao có mài mới sắc, người có học mới nên
(A knife must be filed to be sharp, a person must study to be skilled)

- stab at the big picture
- role of advanced technology
    - in Vietnam’s economic development
- key role of research and universities

Recent Vietnamese Development

- among fastest sustained economic growth in history
- initial ↑ productivity in ag and family businesses
  - gave land to households & allowed markets
- export growth from foreign investment (FDI)
  - low wages, good basic education and health, trade route access

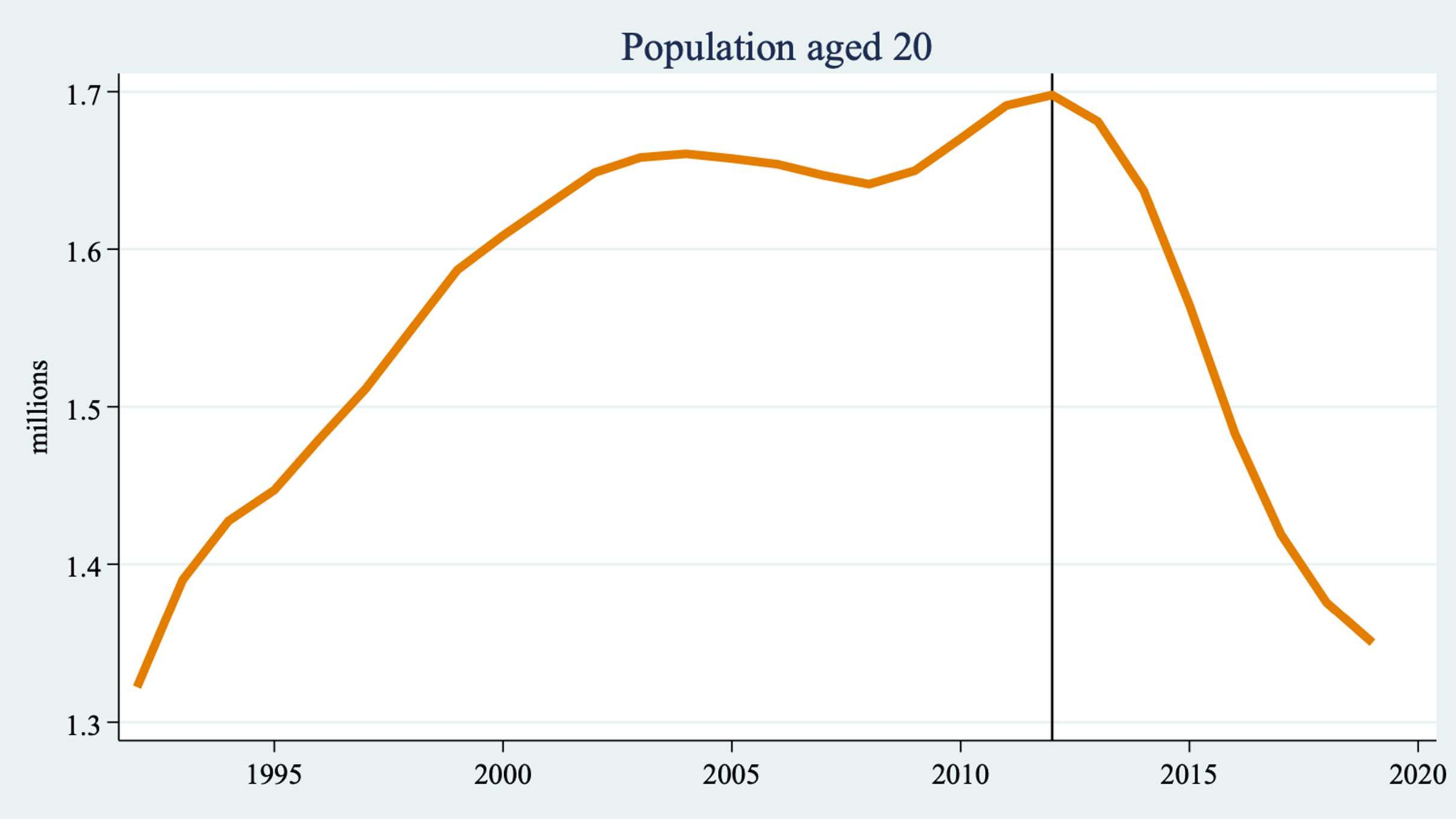


Grew to 5.7 *times*

in 35 years

Low-wage export model losing steam in middle income

- low productivity industries: garments, shoes, basic electronics
  - vulnerable to competition & automation
- wages are rising
- foreign firms not bringing in new technology
  - *e.g.* tracking garments in Hải Dương
- fewer people entering working age


Population aged 20
millions
1.7
1.6
1.5
1.4
1.3
1995
2000
2005
2010
2015
2020

IIC 2022 ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

Middle income challenges

- economy becomes steadily more complex
  - requires flexible and subtle regulation
  - transparent institutions
- transition to higher value-added production
  - supports higher wages

Higher value-added industries

- attract higher productivity exports FDI
  - *e.g.* Intel, Samsung, Apple
  - still rarely innovating in Vietnam
- innovation in private firms
  - *e.g.* VinGroup, FPT
  - some smaller foreign firms

Advanced technology ecosystem

- required for higher value-added production
  - reliable, efficient regulation of private firms
  - access to capital by merit, not connections
  - physical infrastructure (transport, utilities, communications)
  - **intellectual infrastructure** (local expertise)
  - all of these organized by the government

Intellectual infrastructure

- depends on research-focused universities
  - non-research universities lack up-to-date expertise
- required to train engineers, managers, computer & data scientists, etc.
  - Intel Vietnam discovered this was missing
  - why VinGroup and FPT created universities
- pre-condition for high-value niches (Silicon Valley due to Stanford)
  - not successfully selected by governments

Evidence on contribution of higher education

- Vaca Pereira Rocha (2022) cross-country results
  - more tertiary education ⇒ more labor in high-tech manufacturing
  - manufacturing has higher growth potential than services, especially for low income countries
  - high-tech manufacturing has the highest growth potential
  - university education + good conditions for high-tech
    ⇒ faster economic growth

Vietnamese universities

- Soviet model removed research
- grew rapidly but changed little for first 20 years of Đổi Mới
- big changes in past decade
- still not clear if there is a plan to create world-class universities
  - requires incentives, competition, sustained investment
  - surprisingly small investment compared to other infrastructure
    - VN spends > $1 billion/year on U.S. university tuition

Example of China

- until 1999, no universities in top 800 in world
- Project 985 spent $36 m./year extra on 9 universities
    - brought Chinese researchers back to China
    - *e.g.* Nobelist at Princeton given carte blanche to build team
- in 2015, 2 universities in top 50 & 37 in top 800
- crucial to China’s technological advance

Elements of a research university

- faculty’s most important job is research
- all faculty have high quality PhDs
  - pay and working conditions good enough to attract them
- university autonomy from MoET
- research funds should be allocated competitively (e.g. NAFOSTED)
  - to be published in ranked journals
- necessary for credible graduate degree programs
- can start with small institutions

IIC2022
ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT

huge research potential in Vietnam

- disciplined students, well trained in math
- education highly valued by society
- none of my VN grad students plan to work in VN universities
- many great Vietnamese researchers, but few in Vietnam
  - of top 100 Nguyễns, only 21% work in VN, only 11% in VN universities
- VN has created world class high schools - but most leave
  - Amsterdam, Chu Văn An, Quốc Học, Lê Quý Đôn, Lê Hồng Phong

Big advanced technology opportunities for VN

- ABC - anywhere but China
  - Vietnam is a preferred alternative to China
  - since 2018, VN exports to US ↑ 170%
- Apple moving production to Vietnam
  - but iPhone to India - technology not yet sufficient in Vietnam

Automation must not leave workers behind

- raise worker productivity instead of keeping wages low
  - skilled workers are complementary with automation
  - create training and conditions to give workers opportunities
    - e.g. German technical high schools
- if workers are marginalized, automation is not politically sustainable
- regular U.S. workers barely benefited from economic growth for 40 years
  - major cause of current political conflict

Conclusion

- Vietnam has big advanced technology opportunities
- very important for succeeding in middle income stage
- physical infrastructure investments have been mostly good
- intellectual infrastructure investments are late and limited
- strong research universities are feasible, affordable and needed

IIC2022
ADVANCED TECHNOLOGY AND SUSTAINABLE DEVELOPMENT