SECURITIZING INNOVATION TO PROTECT TRADE SECRETS BETWEEN "THE EAST" AND "THE WEST": A Neo-Schumpeterian Public Legal Reading

Riccardo Vecellio Segate

Abstract

The first target of today's global commercial and military espionage, trade secrets, are the only form of intellectual property protection to be based on the necessity of nondisclosure and secrecy rather than on the paradigm of publicity and exploitability, with the obvious consequence that where confidentiality ends, no trade secret factually exists anymore. As such, current judicial remedies to trade secret thefts simply miss the point, treating trade secrets as rights which can be restored, rather than as assets that once stolen, are lost forever. Moreover, trade secrets often represent the "backbone" of a country's development: an invaluable strategic advantage for entire industrial systems, innovation environments, and national economies. Whereas a trade secret theft occurring within domestic borders transfers exploitability rather than causing damage to the economic ecosystem of the country concerned, international trade secret thefts may jeopardize states' economy and public security alike. For these reasons, the only way to protect trade secrets by law is through ensuring that their secrecy is reasonably safe by means of compulsory cybersecurity and cyber-hygiene standards to be complied with by their owners. When it comes to this specific form of IP, the only protection is afforded with prevention: injunctions and compensations can work as remedies for other IP rights' misappropriations and misexploitations, but do nothing to restore the peculiarity of a trade secret which is, indeed, its secrecy. Not only should companies be compelled to adopt and implement reasonable sector-specific IT security measures and procedures, but licensing agreements including know-how should feature a specific cybersecurity clause to be carefully negotiated. The new cybersecurity regimes of world powers like China seem to capture this problem, and to (involuntarily?) provide useful tools for addressing it beyond the schemes of intellectual property or tort (confidentiality) laws. Regrettably, other countries in the Pacific region appear to keep the belief that trade secret thefts are a private affair of the breached companies, which

should seek redress via traditional judicial channels. This is to be deemed an outdated, misleading, shortsighted and ineffective approach.

About the Author

Riccardo Vecellio Segate is the Talent Program Ph.D. candidate at the Faculty of Law of the University of Macau, and a Visiting Fellow at the Centre for Law and Technology at the University of Hong Kong. He was previously an Exchange Scholar at Tsinghua Law School in Beijing, and has just been selected for a visiting position at Berkeley Law starting this Fall. He completed, *inter alia*, a Master of Laws in Public International Law from Utrecht University, a Postgraduate Diploma in European and Global Governance from the University of Bristol, and three Diplomas in European Affairs, Development Cooperation, and Humanitarian Intervention from ISPI in Milan. Vecellio Segate served as the Executive Editor and Secretary of the *Utrecht Journal of International and European Law* in 2017–2019, and worked extensively in policy and legal affairs for both private firms and public institutions all across Europe and Asia. He is also the case-law reporter for Oxford University Press' *International Law in Domestic Courts* Reports, for the jurisdiction of Hong Kong.

Table of Contents

Introduction

Although all companies face the risk of loss of intellectual property and confidential business information, some sectors—finance, chemicals, aerospace, energy, defense, and IT—are more likely to be targeted and face attacks that persist until they succeed. Losses are higher for sectors where it is easier to monetize the stolen data, as with the chemical industry where proprietary formulas can be easily duplicated or with sensitive business information on business negotiations.[1]

As the edge between trade secrets and state secrets keeps blurring across both democracies and authoritarian countries, trade secret thefts increasingly stand halfway between national security and commercial espionage.[2] Perhaps unsurprisingly, in China—where "Western" corporate-oriented ways of dealing with trade secrets were gradually introduced from the late 1980s only—*trade* secret protection overlapped with that of *state* secrets for a very long time.[3] It is worth noticing that these roots might be able to explain why, besides Beijing's "highly

---

* An earlier version of this article was presented on February 1, 2019 at the "First IP & Innovation Researchers of Asia (IPIRA) Conference" organized by the University of Geneva, WIPO and WTO, held at Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, in Kuala Lumpur. On that occasion, I benefitted from sharply provocative comments by Professor Glynn S. Lunney, Jr. and Professor Nari Lee. Refined drafts have subsequently been delivered at the Regional Convening of the Young Scholars Initiative organized in Hanoi on August 14, 2019, as well as at the 7th Biennial Conference of the Asian Society of International Law, held in Manila on August 22, 2019, and at the 10th Asia-Pacific Innovation Conference held at the School of Economics of Peking University (Beijing) on October 11, 2019. Comments are most welcomed, and can be addressed to *r.vecelliosegate@connect.um.edu.mo*. All links are live and accurate at the time of publication. The law is updated by October 2019. No funding was allocated to this research, and no conflicting interest conditioned my methodology, approach, findings, or beliefs.

1. Chiara Gaido, *The Trade Secrets Protection in U.S. and in Europe: A comparative study*, 24(2) Revista La Propiedad Inmaterial 129, 132 (2017).

2. Peter K. Yu, *Trade Secret Hacking, Online Data Breaches, and China's Cyberthreats*, Cardozo Law Review de novo 130, 133–134 (2015). *See e.g.*, the vicissitudes of Mr. "Khan, a German-educated metallurgist, [who] left the Urenco enrichment facility at Almelo, The Netherlands, taking with him uranium enrichment design blueprints. He returned to his home in Pakistan and began a covert nuclear weapons program that would be known as the Dr. A. Q. Khan Research Laboratories (KRL). This ultimately led to the successful detonation of Pakistan's first nuclear device on May 28, 1998. . . . Not only did Khan proliferate nuclear centrifuge trade secrets to his country, but the Khan network expanded to include technology transfers to Iran, Libya, North Korea, Iraq, Saudi Arabia, Sudan, Nigeria, Malaysia, Indonesia, Algeria, Kuwait, Myanmar, Brazil, and possibly Syria, Egypt, South Africa, Turkey, and other South American countries. It is also suspected that workable designs for a nuclear warhead were sold to Libya and several other countries." David York, *Illicit Trafficking in Nuclear and Radiological Materials*, *in* National Security Issues in Science, Law, and Technology 75, 79–80 (Thomas A. Johnson ed., 2007).

3. Ping Xiong, *China's Approach to Trade Secrets Protection: Is a Uniform Trade Secrets Law in China Needed?*, *in* The Internet and the emerging importance of new forms of intellectual property 251, 252; 256–262 (Susy Rebecca Frankel & Daniel J. Gervais, ed., 2016).

questionable" intellectual property rights (IPR) records in its international relations (including alleged state-backed trade secrets thefts),[4] China can be deemed today to stand as the most advanced domestic system of trade secrets protection in the world. If IP is truly the US' foreign affairs priority in international cybersecurity governance,[5] then it is worth exploring whether the West should protect its business assets (at least externally, i.e. facing international theft) *close to* the way China does[6] domestically: to answer this question, this Article will comment on a few key provisions enacted by the major powers of the Pacific region.

Provided that a trade secret "has commercial value *because* it is secret,"[7] it arguably requires a drastic change of paradigm in the way the law addresses its acquisition and especially its loss. When it comes to trade secrets—unlike any other IP scenario—post-factum remedies are *not* a solution: the only reasonably useful role the law can play is to regulate preventive measures and the balance between private and public actors in charge thereof. Anyone developing a product similar enough to granted patents, regardless of their awareness about that patent's registration, is a patent infringer; conversely, the only way to be prosecuted for copying a trade secret is by actually *stealing* and replicating it.[8] Even the information constituting a forthcoming patent, before the latter is granted (thus published), is protected as a trade secret (at least in most jurisdictions, including the United States);[9] similarly, a copyrightable work remains a trade secret until the author/owner goes public about it.[10] However, English prior-use

4. *See generally* Carl Roper, Trade Secret Theft, Industrial Espionage, and the China Threat (2014).

5. Nir B. Kshetri, The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies 62 (2016).

6. Interestingly, such way is nothing else than having learnt to play by our own Eurocentric rules; indeed, "[n]otable civilizations, including Imperial China, the Arab world, and undocumented pre-historic indigenous and local communities across the globe sustained their distinguished technological and scientific feats without a conventional intellectual property system. Also, the customary legal regimes that promote creativity in indigenous and local communities are far from being regimes of exclusion like the conventional or western forms of intellectual property." Chidi Oguamanam, *Beyond Theories: Intellectual Property Dynamics in the Global Knowledge Economy*, 9 Wake Forest Intell. Prop. L.J. 104, 119 (2009).

7. Agreement on Trade-Related Aspects of Intellectual Property Rights Art. 39(2)(b), Apr. 15 1994 Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 187. [hereinafter TRIPS Agreement].

8. Herbert J. Hovenkamp, *Antitrust and the Patent System: A Reexamination*, 76(3) Ohio State L.J. 467, 501; 559 (2015).

9. Gil Ohana & C. Bradford Biddle, *The Disclosure of Patents and Licensing Terms in Standards Development*, *in* The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents 244, 249 (Jorge L. Contreras ed., 2018).

10. Notably, "to gain the advantages of a state-backed property right, some of the advantages offered by a regime of free contract must be sacrificed. Some agreements possible under the latter system will be unenforceable under the former. . . . In intellectual property, for example, a party could lose some degree of contractual freedom when it abandons a trade secret in favor of a copyright or patent." Robert P.

doctrine specifies that if third parties were using the next-to-be-patented invention secretly (as a trade secret), they cannot prevent that patent from being issued; this is because patents are "granted to the first to file and disclose the invention rather than the first to invent."[11] In sum, once a trade secret is stolen, patentability is difficult to prevent.[12]

Dual-use technologies feature in the trade secret-protection arsenal of civilian corporations as much as dictatorships and military regimes all around the globe.[13] When one can no longer ignore the interfaces amid intellectual property rights, cybersecurity policing, competitiveness, and state economic securitization of cyber-exposed trade secrets, a purely legalistic approach to cyber-enabled trade secret misappropriation cannot stand in a vacuum. Citing evidence that many trade secret misappropriation incidents are tied to cybersecurity vulnerabilities and consequent breaches,[14] this Article makes a case for the public value of protecting trade secrets by preventatively securitizing[15] companies' IT networks and abandoning the old-fashioned legal approaches placing post-factum responsibilities under the light. Trade secrets thefts mean *loss* or—a far worse geopolitical consequence—*transfer* of state socioeconomic and political-military assets, which represents a collective damage far exceeding the financial hurdles it entails for the single manager or entrepreneur.

"Legislators have felt compelled to create new statutes to address these problems, but the analytical difficulties that computers presented to law enforcement continue to grow."[16] Whereas the prevalent approach in today's national "trade secret strategies" is for the State to "soft support"

Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of On-line Commerce*, 12(1) Berkeley Tech. L.J. 115, 121 (1997).

11. Lionel Bently & Brad Sherman, Intellectual Property Law 638 (4th ed. 2014).

12. However, as far as the United States is concerned, read the implications of the 2012's Leahy-Smith America Invents Act. Brian J. Love & Christopher B. Seaman, *Best Mode Trade Secrets*, 15(1) Yale J. of Law and Tech. 1 (2013).

13. *See, e.g.*, Herbert S. Lin, *Governance of Information Technology and Cyber Weapons*, *in* Governance of Dual-Use Technologies: Theory and Practice 112 (Harris et al. eds., 2016); Helena Legarda, *China's pursuit of advanced dual-use technologies*, International Institute for Strategic Studies (Dec. 18, 2018), https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance. [https://perma.cc/M4QY-YYYG].

14. Ignacio De Leon & Jose Fernandez-Donoso, Innovation, Startups and Intellectual Property Management: Strategies and Evidence from Latin America and other Regions xvi; 97–98 (2017).

15. Securitization is employed in this work under the international relations (IR) acceptation of the term, and not under the finance or economics one. It concerns extraordinary (and *prima facie* overdemanding) security-based measures adopted in domestic and international legislation to face exceptionally severe, new, urgent or threatening situations. For an application of this IR meaning to legal disciplines. *See* Wouter G. Werner, *International law: Between legalism and securitization*, *in* Security: Dialogue Across Disciplines 196 (Philippe Bourbeau ed., 2015).

16. Aaron J. Burstein, *A Survey of Cybercrime in the United States*, 18(1) Berkeley Tech. L.J. 313 (2013).

private cybersecurity initiatives (if anything),[17] that support does not suffice when not complemented by binding standards for corporations to meet. In a sort of cybersecurity-by-design scheme, companies should be required *by law* (hard provisions) to comply with preset cybersecurity standards in-house, and be bound to include and implement cybersecurity clauses in licensing agreements[18] also concerning or encompassing trade secrets, whereby the licensee guarantees the licensor the respect of certain cybersecurity standards (*a fortiori* in nonexclusive or sole licensing transactions, and including the compulsory ones). Incompliant companies should be fined on the model of the "U.S. Federal Trade Commission, which brings legal action against companies that sell devices with insufficient data security features."[19] This way, trade secrets will retain the whole of their virginal "informational wealth". The rationale is necessary not only to prevent disruptions to States' national economy due to innovation jeopardy, but it is also needed because the nonprevention of trade secret thefts may go so far as to engage the international responsibility of the State concerned if companies or their officers are expressions of that State's apparati to a sufficient degree. Regarding this last claim, an international requirement that States adopt domestic laws to mitigate the externalisation of cyberattacks impacting their companies' trade secrets should be introduced in relevant international treaty law.[20] Indeed, in an aggregated sense, those trade secrets can be rethought about as "public goods".

"Securitizing" cybersecurity policing is not per se tremendous news in literature;[21] however, no analysis has been carried out to date in order to frame this securitization against a political economy perspective that

17. *See, e.g.*, the U.S. one: Exec. Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (2013) https://obamawhitehouse.archives.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [https://perma.cc/KKY9-EDRY].

18. This is already a suggested—but unfortunately, not standard—practice in the sector; *see* Jason Howg, *Unique Trade Secret License Agreement Features*, Lexology (Mar. 31, 2017), https://www.lexology.com/library/detail.aspx?g=4c07d1b3-b37c-490d-8b43-d0d8e64bdf7c [https://perma.cc/CP2V-JCSZ]. Exactly because it is not yet widely adopted and attacks are increasing exponentially in both frequency and scope, a binding approach by the legislator is rather called for.

19. Lothar Determann, Determann's Field Guide to Data Privacy Law 145 (2017).

20. For example, in the law of the World Trade Organization (WTO), or as an update to international commercial law conventions promoted by the United Nations Commission on International Trade Law (UNCITRAL), such as the 1980 UN Convention on Contracts for the International Sale of Goods (CISG) or even, more tangentially, the 2005 UN Convention on the Use of Electronic Communications in International Contracts (ECC). Similar considerations are valid for regional arrangements like the European Union (EU), as well as for free trade areas and bilateral investment agreements (by proceeding in the way that will be partly elucidated *infra*).

21. *See, e.g.*, this short opinion piece: R. Mark Halligan & Richard F. Weyand, *Cybersecurity, Trade Secret Asset Management and the Defend Trade Secrets Act of 2016*, LinkedIn (Jul. 21, 2018), https://www.linkedin.com/pulse/cybersecurity-trade-secret-asset-management-defend-secrets-halligan [https://perma.cc/BW9U-LTHX].

placed special emphasis upon the public significance of "innovation through IP protection" as a social asset to be pursued and defended collectively. No emphasis has been placed on the interfaces between trade secrets as innovation assets and as security assets, either, although this overlap is crucial: when trade secrets are algorithms, for instance,[22] their stealing provides the thieves not only with the algorithms themselves, but even more importantly, with their underlining machine-learning data used until then to operate and improve (and that data may disclose sensitive patterns on the concerned population's features, habits, beliefs, etc.). Similarly, there is no comparative[23] analysis which, taking the US legislation as the benchmark,[24] has focused on the Indo-Pacific region[25] and its four main players.[26] Critics of *general IP* securitization have complained that

22. On algorithms protected as trade secrets from a public policy perspective, see the relevant video records. *Conference on Trade Secrets and Algorithmic Systems*, New York University (Nov. 2018), https://www.law.nyu.edu/centers/ili/events/trade-secrets.

23. The reader is welcomed to be noted that the present work does *not* aspire to be "comparative" in the proper sense of the term. It rather illustrates policy, legal and economic angles of a complex problematic and puts forward a kaleidoscope of ideas on how and why they should be addressed, drawing from the positive or negative experiences of the top players in the chosen region, by outlining selected similarities and divergences among them.

24. This is not a choice of scholarly ethnocentrism: in this field, U.S. law objectively shaped concepts and methodology *deliberately* imported within several jurisdictions across the other shore of the Pacific. For a similar analysis (targeting South Korea) on East-imported trade secrets, *see* Hyun-Soo Kim, Trade Secret Law, Intellectual Property, and Innovation: Theoretical, Empirical, and Asian Perspectives (2010) (LLD Dissertation at the University of Illinois at Urbana-Champaign). Also, one should be mindful of the standard-setting role played internationally by the US (more generally about IP) during the TRIPS negotiations. S*ee* Peter Drahos, *Developing Countries and International Intellectual Property Standard-Setting*, 5 Journal of World Intell. Prop. 765, 771–772 (2002).

25. "Indo-Pacific" is used here to refer to the "Indo-Pacific" and "East Pacific" regions at the same time, i.e. to the area-arch roughly extending from New Zealand to India to Japan.

26. The choice for these four "main" jurisdictions (Australia, Mainland China, India, and Japan) is to an extent subjective, but not arbitrary; in fact, it is based on a multifaceted balance between numerous economic, sociolegal, political, entrepreneurial and demographic selection criteria, including: population size, total GDP nominal, total GDP PPP, GDP nominal per capita, GDP PPP per capita, regional diversity, public research expenditure, annual growth rate, developmental stage, innovation capacity, technology diffusion, internet penetration, and geopolitical influence both within and beyond the region. To exemplify, if GDP per capita figures were to be preferred, India would have been excluded; similarly, if greater emphasis was placed upon annual growth rate, Indonesia would have been selected, and if core innovation parameters were accorded higher preference, South Korea would have been included before all others. On balance, we believe that the four chosen jurisdictions overall are duly reflective of the similarities, differences, and "cross-contaminations" in the legal protection of trade secrets which matter the most for the sake of this analysis. Nonetheless, a few considerations shall be spent on what is probably the most important among the unexamined countries: South Korea, widely considered top-tier globally for innovation performance (refer to: Bloomberg Innovation Index 2020, WIPO/

"the theft of intellectual property as a security issue helps justify enhanced surveillance and control over the Internet and its future development[, with] the uncritical acceptance of the IP theft narrative at all levels."[27] Besides undue generalizations, this claim encapsulates some truth. Hence, this Article will tailor its arguments to the stealing of trade secrets only; importantly, it will not advocate for an enhanced *direct* role of the State, but rather for "responsibilization policing" about companies themselves, with particular care for the smallest and most innovative ones. This way, it will displace the politics of IP exceptionalism and advocate for cybersecurity implementation to become a standardized praxis, towards a sort of "protection-by-design" model. Inspiration to this end can be gained from macroeconomic and public policy literature, and also by drawing appropriate comparisons from relevant international security conventions, as will be demonstrated *infra*.

I. The Ontology and Functionality of a Trade Secret

On both sides of the Atlantic, trade secret law is a niche of the more general unfair competition law, which protects confidential information more comprehensively.[28] Internationally, trade secrets are the only IP

INSEAD Global Innovation Index 2019, WEF Global Competitiveness Report 2018, and BCG International Innovation Index 2009). The following elements are notable about and peculiar to this country's framework concerning trade secrets. First, Article 2(2) of the amendment to the Unfair Competition Prevention and Trade Secrets Protection Act (Act No. 15580 of April 17, 2018) which entered into force on July 9, 2019 provides for relaxed requirements for claimants of an alleged misappropriation, mandating no need for evidence of reasonable efforts to having kept the assets' secrecy. This is virtually a unicum among industrialized nations. Second, Article 14(2) establishes treble damages in civil proceedings, and Article 18 of the same amended Act introduces imprisonment of up to 15 years or a fine of up to KRW 1.5 billion for misappropriation of Korean trade secrets which involves (awareness of) use of such secrets overseas. To summarize, Seoul has gone the extra mile to protect its assets by emphasizing the criminal side of transnational misappropriations and strengthening attention to thefts involving SMEs; yet, considering the lack of an "effort" requirement for a company to demonstrate it maintained its assets secret, the proposal formulated in this Article does not easily fit the Korean protection system. Nevertheless, the most recent version of the Fair Transactions in Subcontracting Act (Act No. 15362 of January 16, 2018) stipulates increased liabilities for technology transfers between major corporations and SMEs, to the effect that large corporations must put in place security standards as to ensure the secrets of small companies are particularly preserved from possible intrusion, alteration, and misappropriation—*see* Jeong Yeol Choe, Samuel SungMok Lee, Hyeong Joo Lim, and Woo Rim Lyu, *Substantial Risks Created for Foreign Companies by New Korean Regulations on the Taking of Technical Materials and Ideas from SMEs*, Lexology (2018), https://www.lexology.com/library/detail.aspx?g=1fedb55f-031e-41f4-abb1-0b11bcdf94fe. For scholarly literature on these legislative developments, *see, e.g.*, Youngsun H. O. Cho, Intellectual Property Law in South Korea (2d ed. 2019); for an older comparative account with the US, refer to the unpublished paper: Mirjana Stanković, *Trade Secrets: South Korea versus United States*, SSRN (2019), https://ssrn.com/abstract=2357385.

27. Debora J. Halbert, *Intellectual property theft and national security: Agendas and assumptions*, 32(4) The Information Society 256, 262 (2016).

28. *See, e.g.*, Katarzyna A. Czapracka, *Antitrust and Trade Secrets: The U.S. and*

protection system (among the major four, the others being patents, trademarks, and copyrights) not to be regulated by a dedicated convention;[29] they have no standing in general IP multilateral treaties, either. This notwithstanding, the TRIPS eventually established the nature of data exclusivity to be that of an intellectual property right,[30] and trade secrets' importance in bilateral arrangements and domestic venues is rapidly on the rise, as they cover fields more and more important to societies (including pharmaceutical products,[31] indigenous knowledge,[32] and climate-change technologies[33]). Although frequently associated with scarce degrees of transparency and accountability (or, perhaps, exactly due to this shortcoming),[34] trade secrets are definitely the most highly valued and reliable type of IP for companies across multiple industries.[35] This is especially true for startups.[36] A trade secret is a piece of information (e.g. a formula, drawing, pattern, software,[37] ingredient, know-how, compilation including a customer list,

the EU Approach, 24:2 Santa Clara High Tech. L.J. 207, 213; 222–226 (2008). Other approaches to trade secrets protection might be those of human rights, breach of confidence (in contract law), labour law, corporation law, martial law, industrial law, marketing law, and law of property. For example, "[w]hen considering reliance on international trade secrets laws, [and] a contract is being considered (e.g., a confidentiality agreement or a more complex business arrangement), [one should consider] providing that enforcement of the secrecy of the confidential information will be in the [relevant domestic jurisdiction]. This [often] provides a contract breach claim in addition to a trade secret theft claim." Eric M. Dobrusin & Ronald A. Krasnow, Intellectual Property Culture: Strategy and Compliance 313 (2017).

29. Protecting the other IP categories are e.g. the Trademark Law Treaty (1994), and the Madrid Agreement Concerning the International Registration of Marks (1891) with its Protocol (1989); the Patent Cooperation Treaty (1970), and the Patent Law Treaty (2000); the Universal Copyright Convention (1952), and the Berne Convention for the Protection of Literary and Artistic Works (1886).

30. Meir Perez Pugatch, The International Political Economy of Intellectual Property Rights 147 (2004).

31. *Id.* at 85–95, 152, 176, 207–210.

32. *See, e.g.*, Deepa Varadarajant, *A Trade Secret Approach to Protecting Traditional Knowledge*, 36(2) Yale J. of Int'l. L. 37 (2011).

33. Jon P. Santamauro, *Failure is not an option: Enhancing the use of intellectual property tools to secure wider and more equitable access to climate change, in* Environmental Technologies, Intellectual Property and Climate Change: Accessing, Obtaining and Protecting 84, 86–87 (Abbe E. Brown ed., 2013).

34. *See, e.g.*, Claude Castelluccia & Daniel Le Métayer, Understanding algorithmic decision-making: Opportunities and challenges 56 (European Parliamentary Research Service 2019).

35. Katherine Linton, *The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research*, Journal of Int'l Com. and Econ. 6–7 (2016).

36. Richard D. Harroch, *10 Intellectual Property Strategies For Technology Startup*, Forbes (Jun. 6, 2016), https://www.forbes.com/sites/allbusiness/2017/06/06/10-intellectual-property-strategies-for-technology-startups/#75ac68a0ab1b [https://perma.cc/AN7N-UYAT]; De Leon, *supra* note 14, at 37.

37. But according to some authors, trade secret law is inadequately placed to protect software. *See, e.g.*, Philip Leith, Software and Patents in Europe, 163–164 (2007). In some jurisdictions, though, relying on trade secrets is de facto the only solution left; in this direction, for the consequences of the 2014's *Alice* decision in the

program, contract, device, method, technique, or standardized process) that independently derives actual or potential economic value from not being generally known, and that is subject to reasonable efforts to maintain its secrecy:[38] even a mathematical formula can be protected as a trade secret![39] Its protection has no time limit, depending on the owners' interest and ability to keep it secret, as much as on third parties' readiness to reproduce it fairly (i.e. without misappropriation).

As secrecy is the most obvious feature of this IP protection system, a notable role of the law is to establish the conditions for demonstrating the existence of such a propriety in the relevant time and market. The United States made a notable turn from reasonable *efforts* (Uniform Trade Secrets Act, 1985) to reasonable *measures* (Defend Trade Secrets Act, 2016),[40] although this last wording already formed part of the Economic Espionage Act (1996).[41] The extent of this "reasonableness" requires a contextualized appraisal of the value of the secret to be kept,[42] the size and/or capabilities of the companies, and other circumstances,[43] but arguably also adaptation to the changing security landscape,[44] which calls for higher and higher standards.[45] Almost anything that is maintained in secret, not generally known to or readily ascertainable by competitors, and provides

US, refer to Samuel J. LaRoque (2017) *Reverse Engineering and Trade Secrets in the Post-*Alice *World*, 66 Kansas L. Rev. 427 (2017).

38. C. Kerry Fields & Henry R. Cheeseman, Contemporary Employment Law 112 (3d ed. 2016).

39. Leith, *supra* note 35, at 142–143.

40. Seth J. Welner & John Michael Marra, *Defend Trade Secrets Act vs. Uniform Trade Secrets Act: Reasonable Security Measures as Objective or Subjective?*, Holland & Knight Trade Secrets Blog (Aug. 6, 2018), https://www.hklaw.com/en/insights/publications/2018/08/defend-trade-secrets-act-vs-uniform-trade-secrets [https://perma.cc/E9X4-PZAM].

41. Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57(2) Boston College L. Rev. 381, 410 (2016).

42. Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17(1) George Mason L. Rev. 1, 10 (2009).

43. TRIPS Agreement, *supra* note 7, at Art. 39(2)(c).

44. For case-law examples of security standards recently upheld by US Courts, *see* Abigail W. Lloyd & Mark P. Wine, *Spring Cleaning: Tidying Up Your "Reasonable Efforts" to Maintain Trade Secrets*, Orrick Trade Secrets Watch (Apr. 26, 2019), https://blogs.orrick.com/trade-secrets-watch/2019/04/26/spring-cleaning-tidying-up-your-reasonable-efforts-to-maintain-trade-secrets [https://perma.cc/88GR-MFDZ]; *see also* Porter Wright Morris & Arthur LLP, *Lack of reasonable efforts to maintain secrecy of trade secrets can undermine otherwise compelling claim of misappropriation*, Technology Law Source (Apr. 23, 2014), https://www.technologylawsource.com/2014/04/articles/intellectual-property-1/lack-of-reasonable-efforts-to-maintain-secrecy-of-trade-secrets-can-undermine-otherwise-compelling-claim-of-misappropriation [https://perma.cc/6Q5T-BBUU].

45. "[R]ules stipulate brighter lines while standards rely on more general criteria. . . . Perhaps the most important and most obvious reason [why] data security rules require flexibility is the inevitability of rapid technological change. Both threats and solutions evolve too quickly to keep precise rules up to date." William McGeveran, *The Duty of Data Security*, 103(3) Minnesota L. Rev. 1135, 1197–1198 (2019).

a competitive advantage is potentially protectable via trade secret.[46] For instance, the Coca-Cola recipe is the most obvious example of a trade secret within the food industry. We must therefore reject the postulation that "[s]ince taking knowledge is much easier than putting it to use, theft of trade secrets has had a relatively limited impact on competitive economic development."[47] To the contrary, this is only true as far as a limited number of technology-intensive secrets are concerned. Trade secrets protect R&D research,[48] marketing efforts, strategic planning, and information that may not be protected by patents, trademarks, or copyrights. Unfortunately, it is difficult to address legally, as trade secret status is applied automatically, with no government entity in charge of delivering a first assessment. Expected efforts to secrecy maintenance may include IT security, physical infrastructural security, and advanced confidentiality screening of human personnel involved in data handling (i.e. data transferring, processing, systematisation, etc.). "If the secret is embodied in an innovative product, others may be able to . . . discover the secret and be thereafter entitled to use it. Trade secret protection of an invention in fact does not provide the exclusive right to exclude third parties from making commercial use of it. Only patents and utility models can provide this type of protection."[49] Despite this apparent lack of formal guarantees, most companies stay away from the more "institutionalized" patenting because not every invention is patentable, and obtaining a patent requires full disclosure. In addition, unlike patents, trade secrets can be kept for as long as needed. The only drawbacks are that first, once made public, they no longer serve their purpose, and second, they do not protect against later matching independent development or accidental disclosure. All in all, it shall also be stressed that trade secrets are *not* alternative to patenting: most patents require some degree of know-how to be successfully "operated." This may explain the empirical concession that "the importance of secrecy [for a company] increases with [the] number of patents held."[50]

Multiple inventions and, more frequently, reverse engineering,[51] increasingly compel corporate lawyers to include nondisclosure as well

46. For two comprehensive yet introductory readings, *see* Brian T. Yeh, Protection of Trade Secrets: Overview of Current Law and Legislation, (Congressional Research Service of the United States of America 2016); Martin J. Salvucci, *A Federalist Account of the Law of Trade Secrecy*, 29(1) Stanford L. and Pol'y. Rev. 183 (2018).

47. Halbert, *supra* note 27, at 261.

48. Aliisa Siivonen, Trade Secret Misappropriation Through Cybercrime: Analysing prohibitions of trade secret misappropriation and cybercrimes in the Criminal Code of Finland, 15 (2018) (LL.M. Thesis in Law and Technology at Tilburg University Law School).

49. *Frequently Asked Questions on Trade Secrets: SMEs*, WIPO (last visited 2019), https://www.wipo.int/sme/en/faq/tradesecrets_faqs.html [https://perma.cc/XX9E-Q587].

50. David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?*, 94(2) Notre Dame L. Rev. 751, 798 (2018).

51. Jim Chen, *Biodiversity and Biotechnology: A misunderstood relationship*, Mich. St. L. Rev. 51, 77 (2005).

as noncompete clauses in employment contracts,[52] *a fortiori* so given the legalization trend of reverse engineering.[53] Also, "keeping secrets secret" seems increasingly improbable with companies under siege worldwide due to an intense wave of cyberattacks.[54] Although larger companies may be able to play it safer on the economics of scale due to their budget and human resources, they are also more vulnerable to certain kinds of attacks. "As shown by works in game theory applied to cybersecurity . . . , in some cases hackers only need to find one weak link in their target's IT systems to succeed, whereas defenders have to cover all bases ('attack anywhere/defend everywhere' model)."[55] Thus, although cybersecurity considerations can shift entrepreneurs' preference from trade secrets to patents (when possible),[56] it must be factored in that large corporations are as prone to be attacked as small companies, for different reasons. What matters is the degree of innovation guarded by those companies' trade secrets: all considered, innovative startups may be deemed to represent the perfect cost-effective target for cybercriminals looking for this kind of IP. In their

52. Richard J. Cipolla Jr., *A Practitioner's Guide to Oklahoma Trade Secrets Law, Past, Present, and Future: The Uniform Trade Secrets Act*, 27(2) Tulsa L. Rev. 137, 150 (1991).

53. *See e.g.* Art.3(1).2.b of the new Trade Secrets Protection Act (*Gesetz zum Schutz von Geschäftsgeheimnissen—GeschGehG*) which came into force in Germany with the release of Federal Law Gazette dated April 25, 2019. The Act implements the EU Trade Secrets Directive 2016/943, whose Art.16 stipulates that "[r]everse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed."

54. John Gelinne et al., *The hidden costs of an IP breach: Cyber theft and the loss of intellectual property*, Deloitte Insights (Jul. 25, 2016), https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html [https://perma.cc/6UUN-GHS4].

55. Claudia Biancotti, *The price of cyber (in)security: Evidence from the Italian private sector*, Questioni di Economia e Finanza—Occasional Papers 10 (2017); *see* also James Rodman Barrat, Our Final Invention: Artificial Intelligence and the End of the Human Era 249 (2013).

56. John Villasenor, *Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur*, 43(2) American Intell. Prop. Law Association Q. J. 329, 354 (2015). Particular emphasis must be placed on one point. "Recent changes to U.S. patent law have worsened the potential consequences of cybersecurity breaches that could allow a competitor to steal information relating to inventions not yet patented. . . . Under the America Invents Act (AIA), the United States moved from a "first-to-invent" patent system to what is called, only partially accurately, a "first-to-file" system. . . . This new landscape gives unethical competitors an increased incentive to extract information about undisclosed inventions that have not yet been the subject of patent filings by the legitimate owner, and then to quickly file patent applications based on the stolen information. This could involve breaking into a company's networks to obtain documents describing inventions under development, and then using those documents to create patent filings that the company responsible for the cyber-attack would claim as its own. . . . [T]he longer a company sits on a new invention without filing a patent application, the more opportunity this gives to both ethical competitors who might independently conceive and file for a patent on the same invention, and to unethical actors who might steal it." *Id.* at 350–352.

fight against cybercriminals, law enforcement agencies are playing an endless game of catch-up,[57] and startups are the most vulnerable losers.

II. The Socioeconomic Costs of an IP Cyber Theft

Too many domestic jurisdictions have relatively new or newly standardized general IPR regimes (influenced by international regimes like WTO), which hardly address cyberspecific IPR governance. With online data extortion on the rise[58] and the Internet of Things predicated to make vehicles more cloud-integrated[59] as much as individuals more device-dependent (thus equipping hackers with additional targets),[60] this is definitely a shortsighted approach.

By way of exemplification, India believes that the discussions and negotiations pertaining to data should be held within the context of the [WTO]. "Data is a new form of wealth," the Foreign Secretary said, adding that the WTO is framing international rules on this issue.[61]

Quantifiers speak loudly: the share of the economy characterized by intellectual property has grown exponentially since the 80s. The total value of US intellectual property in 2012 was estimated at 5.5 trillion US$, equivalent to the 39 percent of its GDP; in other words, the IP-intensive sector grew exponentially even if compared to the overall economic trends, and continues to grow.[62] Relatedly, a May 2013 report from the Commission on the Theft of American Intellectual Property claimed that annual losses to the American economy due to international IP theft were likely over $300 billion (~2% US GDP) and 2.1 million jobs annually.[63] The accurate magnitude of digital crime is not known, but it has been

57. *See, e.g.*, Ben Hayes et al., The law enforcement challenges of cybercrime: are we really playing catch-up?, (Study for the European Parliament 2015).

58. Yujing Liu, *Prepare for more cyberattacks involving extortion this year, Hong Kong information security watchdog warns*, South China Morning Post (Jan. 18, 2018, 3:00 PM), https://www.scmp.com/news/hong-kong/economy/article/2129511/prepare-more-cyberattacks-involving-extortion-year-hong-kong.

59. Carsten Maple, *Security and privacy in the internet of things*, 2(2) Journal of Cyber Pol'y. 155, 170 (2017).

60. Rowe, *supra* note 41, at 405.

61. Shubhajit Roy, *G-20 Osaka summit: India refuses to sign declaration on free flow of data across borders*, The Indian Express (2019).

62. See all relevant figures and statistics in the 2012 'Intellectual Property and the U.S. Economy' Report: U.S. Econ. and Stat. Admin. & U.S. Pat. and Trademark Off., Intellectual Property and the U.S. Economy: Industries in Focus (Mar. 2012), https://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf. See also its 2016 update: U.S. Econ. and Stat. Admin. & U.S. Pat. and Trademark Off., Intellectual Property and the U.S. Economy: 2016 Update (Sep. 2016), https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf. For a critical problematization of this data, refer to Jeremy de Beer, *Evidence-Based Intellectual Property Policymaking: An Integrated Review of Methods and Conclusions*, 19(6) The Journal of World Intell. Prop., 150–177 (2016).

63. *See* the Report: Dennis C. Blair & Jon Meade Huntsman Jr., Report of the Commission on the Theft of American Intellectual Property (National Bureau of Asian Research 2013), http://www.ipcommission.org/report/

estimated that the losses sustained from such attacks amounted to about $1 trillion just for 2010. This estimate compelled Sheldon Whitehouse, a US senator, to echo National Security Agency (NSA) director Keith Brian Alexander[64] and insinuate that the US and the entire world are experiencing what is possibly the greatest transfer of resources through theft and piracy in the entire evolution of mankind.[65]

Insiders' misconduct and inattention are equally dangerous,[66] with employees unauthorizedly accessing data and leaving personal devices unprotected,[67] *a fortiori* when the devices are connected to the corporate intranet.[68] After three former employees of the US medical drug corporation Eli Lilly were charged on a federal indictment of dispatching confidentially-owned information to a rival Chinese firm,[69] the public prosecutor dealing with the lawsuit asserted the stealing as an offense *against the country*.[70]

> Following a number of allegations of state-sponsored hacking, the US recently filed charges including economic espionage against five Chinese military officers for stealing industry secrets on nuclear and solar power. The landmark charges are the first instance of a

IP_Commission_Report_052213.pdf; and its 2017 update: Dennis C. Blair & Jon Meade Huntsman Jr., Report of the Commission on the Theft of American Intellectual Property (National Bureau of Asian Research 2017), http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf). See also the IP Commission's recommendations issued in 2018: Dennis C. Blair & Craig Barrett, Recommendations Regarding the Trump Administration's Section 301 Investigation (2018), http://www.ipcommission.org/report/IPC_Recommendations_to_Section_301_Investigation_March2018.pdf; and updated one year later: Dennis C. Blair & Craig Barrett, IP Commission 2019 Review: Progress and Updated Recommendations (2019), http://www.ipcommission.org/report/ip_commission_2019_review_of_progress_and_updated_recommendations.pdf.

64. Dennis C. Blair & Jon Meade Huntsman Jr., Report of the Commission on the Theft of American Intellectual Property 11 (National Bureau of Asian Research 2013).

65. *See* Press Release, U. S. Senator Sheldon Whitehouse, Whitehouse Delivers Cybersecurity Recommendations for Trump Administration (May 1, 2017). For contextual background, *see* Kshetri, *supra* note 5, at 83.

66. Zak Doffman, *Forget Russia, China And Iran, Up To 80% Of Cybersecurity Threats Are Closer To Home*, Forbes (Apr. 11, 2019), https://www.forbes.com/sites/zakdoffman/2019/04/11/forget-russia-china-and-iran-up-to-80-of-cybersecurity-threats-are-closer-to-home/#62b573ac7eb3; Halbert, *supra* note 27, at 265.

67. Bryan Watkins, The Impact of Cyber Attacks on the Private Sector 5 (AMO Research Center 2014).

68. *Id.* at 3.

69. *See* Justin K. Beyer, *Two former Eli Lilly scientists accused of stealing $55 million in trade secrets*, Lexology (Oct. 28, 2013), https://www.lexology.com/library/detail.aspx?g=8bb4cf35–153c-47e2-bf9e-8185aafcae42 [https://perma.cc/D8G6-FKCT].

70. José P. Sierra, *Lilly scientists prosecuted for trade secret theft*, Lexology (Oct. 17, 2013), https://www.lexology.com/library/detail.aspx?g=653c6a4d-6c69–412a-9cbf-5f286729ff3c [https://perma.cc/K63K-D4UH].

> government formally accusing another nation of cyber espionage and may prove significant for international cybercrime law.[71]

Corporate espionage and the theft of trade secrets, particularly from overseas,[72] represent a growing threat to the U.S. business ecosystem. Some claim their scale equates to that of a war, others rebut that these hyperbolic grievances do not help find solutions to the real issues at stake;[73] whichever the contended numbers, terminology may lead us to frame the problem differently.[74] For example, "data loss" describes the exposure of proprietary, sensitive, or classified information through either data theft or data leakage, but the mainstream rhetoric uses to employ a "warfare" lexicon, by focusing on the theft only.

> The rhetoric of war can also be a political marketing tool used to persuade the public to support certain public policy issues. Along with the "War on Drugs" we have had the "War on Poverty," the "Cold War," and the "War on Terror." . . . [I]t is important to consider the effect that the marketing and presentation of the problem might have not only on the public, but also on policymakers and stakeholders. It is also very important that such rhetoric not stifle or inhibit debate in the exploration of various viewpoints on the issue.[75]

Indeed, the role of companies gets lost in this linguistic and practical overreliance on governments, whereas instead the former should bear primary responsibility.

"Not only are putative trade secret owners required to take reasonable efforts to protect their trade secrets, but . . . [w]hatever metaphorical war might be waging between the government and its enemies, there is no substitute for building stronger defenses in the private sector;"[76] this holds true whether the enemy is an outsider or an insider, as "[c]ompanies cannot afford to rely on the government *or on law enforcement* to stem cyber misappropriation of their trade secrets."[77] In terms of cybersecurity, no company should feel immune to attacks,[78] which "have proven to be a force for hacking groups and state-sponsored organizations seeking to level the playing field with competitors"[79] A big corporation is indeed kept

71. Watkins, *supra* note 67, at 2. *See also* Christopher Burgess, *China continues to steal high-tech trade secrets*, CSO (2017), https://www.csoonline.com/article/3198664/china-continues-to-steal-high-tech-trade-secrets.html [https://perma.cc/V759-YCBK].

72. Dennis Robertson & Susan Decker, *Huawei, Accused of Bullying Ex-Worker, Claims He's a Thief*, Bloomberg (Jun. 3, 2019), https://www.bloomberg.com/news/articles/2019–06–03/huawei-and-former-worker-accuse-each-other-of-stealing-secret [https://perma.cc/PM28-7ATS]. This rhetoric has exacerbated during the Sino-American "trade war".

73. Rowe, *supra* note 41, at 382. *See also* Halbert, *supra* note 27, at 261.

74. *See generally* Rochelle Cooper Dreyfuss & Orly Lobel, *Economic Espionage as Reality or Rhetoric: Equating trade secrecy with national security*, 20(2) Lewis and Clark L. Rev. 419 (2016).

75. Rowe, *supra* note 41, at 395.

76. *Id.* at 396.

77. *Id.* at 408 (emphasis added).

78. Villasenor, *supra* note 56, at 330–331.

79. Watkins, *supra* note 67, at 1.

hostage by the vulnerable interconnectedness among thousands of portable and nonportable devices, as well as by uneven degrees of discretion culture, ethical attitude and security awareness of hundreds of employees. "Of the four types of intellectual property[,] trade secrets are typically the most vulnerable because [they] derive value through the very lack of disclosure that helps define them."[80] For these reasons, a hacker is present on a network for a median number of 214 days before being noticed,[81] undetected incidents are business-disruptive to an extent that makes response to detected or suspected attacks less urgent than the implementation of stringent prevention policies.[82] "Even when discovered, there is no reliable method for determining and estimating actual losses. Rather, it is left to each individual company to disclose the amount of its loss, if it chooses to acknowledge or publicly disclose at all."[83] Wary of stereotyped generalizations, it might be true that in what we used to call the "East", private lobbyists are generally less powerful than in the "West", and as such, legislation on cyber-hygiene and incident disclosure can require more of companies (or at least, of the privately managed ones).

Cybersecurity incidents may cause the stealing of trade secrets (for purposes of economic espionage), their manipulation/alteration/reengineering, a combination of the two, or even their destruction. They can take place physically or online and be due to human error, internal fraudulent behaviour, or loss and/or theft of devices; they might even be caused by an ill-intentioned partner with whom the information was previously shared (such information no longer being "(trade) secret" among them). External threats comprise phishing, malware, spyware, ransomware, and techniques of "social engineering"; a combination of these may lead to misappropriation (i.e. wrongful acquisition, disclosure, and/or use) of trade secrets with the intent to benefit a foreign power,[84] to resell it without ownership oversight, and in any case, to ultimately injure the owner of the secret. In the United States, an individual who is caught stealing a trade secret might face substantial financial burden, including the repayment of the actual damage plus civil disgorgement compensation, plus exemplary damages penalties, and IP attorney fees. Despite this, narrowly legal responses to these phenomena, which could be regarded as appropriate when it comes to other types of IP, become of little solace

80. Villasenor, *supra* note 56, at 331.

81. Brian NeSmith, *Avoid These Top Five Cyberattacks*, Forbes Tech. Council (May. 4, 2018, 8:00 PM), https://www.forbes.com/sites/forbestechcouncil/2018/05/04/avoid-these-top-five-cyberattacks [https://perma.cc/SY5H-UNW6].

82. Villasenor, *supra* note 56, at 331–32.

83. Rowe, *supra* note 41, at 386.

84. *See, e.g.*, Ellen Nakashima, *U.S. Said to be Target of Massive Cyber-espionage Campaign*, Wash. Post (Feb. 10, 2013), https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8–6fc1–11e2-aa58–243de81040ba_story.html [https://perma.cc/F8ET-Z33X]; Rowe, *supra* note 41, at 401. Apparently, China's cyberespionage campaign is facilitated by the state ownership of significant portion of the country's businesses.

when trade secrets are involved. Given that, the true added value of a trade secret lies in its nondisclosure, no compensation can repay the loss: once it happened, such loss is definitive and complete. Indeed, if the possible court costs for the violator are high—up to filing for bankruptcy in a few extreme cases[85]—for the breached company, they might be just as fatal. Possible costs include: immediate business-recovery monetary costs; growing cyber insurance premium; reputational costs;[86] branding disaffection;[87] and loss of business intelligence, market competitiveness, and share value[88] (up to 1.5 percent).[89] Lost profits are also difficult to prove in court,[90] and "compensation for loss vindicates a 'sharing' rationale because it compensates only for present loss and forces the owner to share future profits with the wrongdoer."[91] Further, the loss of valuable intellectual property, especially trade secrets, "can significantly decrease the value of a target company to prospective buyers"[92] in knowledge-intensive industries:[93] Several jurisdictions enacted an obligation to disclose past thefts a company suffered, e.g. before M&A operations or

85. *See, e.g.*, Zak Doffman, *China's Spies Accused of Stealing EU Tech Secrets, Just as China and EU Agree Stronger Ties*, Forbes (Apr. 11, 2019, 8:03 AM), https://www.forbes.com/sites/zakdoffman/2019/04/11/chinese-spies-accused-of-major-european-ip-theft-just-as-china-and-europe-agree-stronger-ties/-a6b8ff070f45 [https://perma.cc/4QKQ-2CL9].

86. *See* Stewart Baker & Melanie Schneck-Teplinsky, *Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US*, *in* Cybercrimes: a Multidisciplinary Analysis 239, 256 (Sumit Ghosh & Elliot Turrini eds., 2011).

87. Raoul Galli, *The Social Life Of Brands: on Choosing Values for Visions (and Divisions)*, *in* Transparency in a New Global Order: Unveiling Organizational Visions 59, 72 (Christina Garsten & Monica Lindh de Montoya eds., 2008).

88. Biancotti, *supra* note 55, at 18.

89. Watkins, *supra* note 67, at 1.

90. *See, e.g.*, Jay Dratler, Jr., *Trade Secrets in the United States and Japan: A Comparison and Prognosis*, 14 Yale J. Int'l L., 68, 102 (1989).

91. Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92(7) Tex. L. Rev. 1803, 1822 (2014).

92. Richard D. Harroch et al., *Data Privacy and Cybersecurity Issues in Mergers and Acquisitions: A Due Diligence Checklist to Assess Risk*, Forbes (Nov. 11, 2018, 2:30 PM), https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/-4e6cf65a72ba [https://perma.cc/H43B-EBF6].

93. "[A]n increase in trade secret protection generates two countervailing effects. On one hand, following an increase in trade secret protection, firm market value increases when targets operate in industries with higher knowledge-worker mobility. On the other hand, firm market value decreases when targets operate in industries with high resource–value uncertainty and high risk of poor investments. . . . [R]egulations promoting stronger trade secret protection do not automatically translate to greater firm value. In particular, when targets operate in less predictable and uncertain industries or in industries where the risk of bad deals is particularly high, a policy that aims to protect trade-secret-related knowledge assets, and therefore to increase their value, might paradoxically reduce the value of the firm in the context of the market for corporate control." Francesco Castellaneta et al., *Money secrets: How Does Trade Secret Legal Protection Affect Firm Market Value? Evidence from the Uniform Trade Secret Act*, 38 Strategic Mgmt. J. 834, 849–50 (2016).

work-for-equity agreements (exceedingly—and increasingly, after the 2008 financial crisis—popular in startup businesses).

As critical cyber infrastructures are frequently managed by private entities even when owned by governments,[94] the latter "must incentivize the [former] to share information and allocate greater resources for security."[95] In so doing, they may decide to frame their policies as either state security–related or innovation-propelling, in accordance with their own prevailing national narratives. In either event, it shall not be forgotten that trade secrets are a pillar of economic growth worldwide. It must not be forgotten, either, that businesses—especially the innovative and small to medium size ones—are networked in IT (intranet) or profit (supply-chain) clusters, which rapidly externalise and spread the cybersecurity issues of each node or the economic fault resulting therefrom. "The vulnerability [of one link-in-the-chain] can create a back-door access to proprietary information, placing the entire supply chain at risk."[96] Extreme cases include governmentally outsourced activities,[97] private-public-partnerships,[98] and technology transfers (defined as "the process by which governments, universities, and other organizations transfer inventions, knowledge, or materials subject to IP restrictions amongst themselves"[99]). Legally, this translates into the advisability of issuing legislation about the lack of due diligence exercised by companies which possess economically fundamental trade secrets and yet do not put in place adequate cyber-resilience policies. Nowadays, leaving devices unprotected equates to exposing one's business, and all its more or less formally "affiliated" ones, to obvious threats which probably cannot be fully avoided, but surely can be mostly circumvented or contained. A too often neglected side-effect of underprotecting those devices is that together with the trade secret per se, sensitive data belonging to business runners and consumers alike, stored on or transmitted through such devices, may be targeted or incidentally found *en passant*, thus exposed to high risks (disclosure, manipulation, etc.). In other words, there are situations where the trade secret coincides at least partially with personal data, so that its unprotected exposure places its holder in breach of relevant data protection laws. This applies, for instance, to certain recorded user habits, customer lists, or potentially very private

94. *See* Ashton B. Carter& Jane H. Lute, *A Law to Strengthen Our Cyberdefense*, N.Y. Times (Aug. 1, 2012), https://www.nytimes.com/2012/08/02/opinion/a-law-to-strengthen-our-cyberdefense.html [https://perma.cc/VCS8-A2DJ].

95. Watkins, *supra* note 67, at 6.

96. Rowe, *supra* note 41, at 423. *See also*, Siivonen, *supra* note 48, at 6.

97. Aaron Gregg, *Amazon Launches New Cloud Storage Service for U.S. Spy Agencies*, Wash. Post (Nov. 20, 2017, 2:26 PM), https://www.washingtonpost.com/news/business/wp/2017/11/20/amazon-launches-new-cloud-storage-service-for-u-s-spy-agencies [https://perma.cc/FB86-GJEU] (United States's top spying service, the National Security Agency, is transferring all its intelligence data to private servers hosted by Amazon).

98. Watkins, *supra* note 67, at 3–4.

99. Intellectual Property and Cyber Law, Pub. Serv. Jobs Directory, https://www.psjd.org/Intellectual_Property_and_Cyber_Law [https://perma.cc/298L-63FU].

identity details related to commercial transactions, partnerships, and agreements. The result is that the holder of the "thieved secret" (or the owner/processor of—or otherwise responsible for—the overlapping "breached personal data") might face serious legal consequences, as the judiciary will then need to make recourse to case-specific balancing exercises whose outcomes are by definition unpredictable. In EU law, for example, the matter is still addressed with significant degrees of uncertainty, since "no discipline prevails *a priori* on the other one";[100] what remains true is that "the application of 'trade secret' law is not sufficient to protect the data protection rights of data subjects, also because the interests and scopes of trade secret protection [as it is currently conceived and designed] are very different from the data protection ones."[101]

To summarize, the "precautionary" approach proposed in this Article would contribute to enhancing data protection and trade secrets protection at once, foundationally, by untangling the just-mentioned dilemma down to its roots and shielding the owner or holder from further responsibilities. Another argument, but on the public side, is that more often than naught, those businesses—however relatively "small" in scale—can play vital functions for the financial sustainability (and thus, even survival) of the State in areas such as defense and energy supply.[102] "IP is the lifeblood of many organizations. It fuels innovation, growth, and differentiation."[103] As such, it must be protected, particularly in its most legally fragile component, trade secrets, which include computer codes and prepatented inventions.[104] "Trade secrets also have a connection to copyright. . . . This was demonstrated in dramatic fashion in late 2014 when cyberattackers breached the systems of Sony Pictures Entertainment and leaked enormous amounts of [unreleased design];"[105] those attacks were most probably state-backed as, unlike common crime, state-sponsored hacking favors longterm dividends.

An additional reason cyber-hygiene should become a priority for business and be mandated by law is that a technical response is not always pursuable, let alone timely. "Canadian telecom giant Nortel Networks Ltd. had been infiltrated by Chinese hackers for nearly a decade before filing for bankruptcy in 2009. The intrusions were so well hidden it took investigators several years to discover the extent of the damage to critical data."[106] In other words, cyber thefts can prove more serious than the physical ones, with limited room for data recovery and disaster management and related

100. Gianclaudio Malgieri, Trade Secrets v Personal Data: A possible solution for balancing rights, 6(2) Int'l Data Privacy L. 102, 104 (2016).

101. *Id.* at 106.

102. Watkins, *supra* note 67, at 2.

103. Don Fancher, *Five Insights on Cyberattacks and Intellectual Property*, Deloitte (2016), https://www2.deloitte.com/us/en/pages/advisory/articles/five-insights-on-cyber-attacks-and-intellectual-property.html [https://perma.cc/8BGU-TR8G].

104. Villasenor, *supra* note 56, at 333.

105. *Id.* at 334.

106. Watkins, *supra* note 67, at 1.

rising insurance costs. Therefore, the "burden of guilt" should shift onto those who should have (reasonably) prevented them well. Cyber intrusions are often anonymized to such an extent that tracing their origin can require several years and an impressive amount of money as well as technical equipment, and ultimately this has no guarantee of success.

III. Shifting the Standpoint

A. *From Private to Public*

"[A]lthough companies have reporting obligations when breaches expose their customers' personal data, they are not generally obligated to publicize intrusions that expose trade secret information unrelated to customer privacy."[107] To make progress workable and fair, this shall change soon: the "public interest" is anyway engaged whenever those companies receive fiscal benefits or are otherwise economically or bureaucratically supported by state institutions. The philosophy behind legal protection of copyrights is to strike the best balance between the need to stimulate creation through grant of copyrights to authors and the need to ensure the interests of the public in accessing information.[108] The opposite holds true with trade secrets: the interest of the public—understood as "social body"—lies in information not to be accessed, from within the public itself but especially from abroad. Traditionally, the public action is oriented towards the establishment of mandatory source code disclosure policies to the benefit of national security, technology dissemination and industrial development, and is complemented by reversed private (e.g. investors) concerns regarding intellectual property protection. The approach proposed here is the abandonment of this unfruitful model, by framing trade secrets' *non*disclosure as an essentially *public* interest. One case stands out for its severity: as trade secrets are the preferred IP protection system for AI innovations,[109] and scientists warn against superintelligence possibly taking over humanity in the foreseeable future if not wisely regulated in time,[110] the industry-led protection of those trade secrets should be a priority under national security strategies and for the governance of security assets nationwide. As "*State-sponsored*

107. Villasenor, *supra* note 56, at 343.

108. Elena Dan, Copyright and Contribution to Knowledge: Towards a Fair Balance of Interests in Knowledge Society 19–25 (2011) (unpublished Master thesis, Lund University) (on file with the Lund University Libraries system).

109. *See* Artem Kocharyan, *Why Intellectual Property is Essential When Dealing with Artificial Intelligence*, Medium (Jan. 13, 2019), https://medium.com/datadriven-investor/why-intellectual-property-is-essential-when-dealing-with-artificial-intelligence-d1372a519eaa [https://perma.cc/7ZU7-5F2H]. *See also* Jessica M. Meyers, Artificial Intelligence and Trade Secrets, A.B.A. (2019), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/january-february/artificial-intelligence-trade-secrets-webinar [https://perma.cc/8CWJ-8766].

110. *See, e.g.*, Michio Kaku, Visions: How Science Will Revolutionize the 21st Century 130–135 (1998). *See generally* Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (2014).

private hackers will be the first to use AI and advanced AI [that is: super-intelligence] for theft,"[111] this imminent threat being global, managing AI-related trade secrets correctly should be a responsibility shared by all nations. One might go as far as to hypothesize an international obligation to that effect.

B. *From Voluntary to Compulsory*

This contribution equally highlights spill-over effects from the data protection and individual privacy regimes to business laws, tailored to the cyberspace. The bulk of this standpoint can be explained as follows. Attributing cyberattacks is admittedly complex, costly, and lengthy. On top of this, the stolen reconceptualized-as-public good (that is, the trade secret) is too valuable to "exit" a country's economy. Formulating provisions binding on companies reverses the forensic or restoration paradigm and seems the only path for the law to impact the above phenomena. Punishing (under tort and, after a certain threshold, even criminally) those who do not adequately prevent (i.e., those responsible for corporate IT systems) as a priority, when compared to those who violated the secrecy of trade secrets, is at first glance a legal heresy; it only makes sense if trade secrets are drastically reconceptualized as a public good entrusted in guardianship by the community to their factual owners. This approach is revolutionary in IP law, but is already at play in the public sector as far as citizens' sensitive data are concerned. A situation in Hong Kong is a good example of this:

> [i]n March 2006, a serious data leakage occurred involving disclosure on the internet of the personal data of some 20,000 people who had lodged complaints against the police with the Independent Police Complaints Council (IPCC). The data included names, addresses, Hong Kong ID card numbers and [criminal records; t]heir leakage, caused by IPCC's *contractor* for computing services, posed an alarming threat to the persons affected.

Thus, the IPCC was found in violation of Data Protection Principle 4 of Schedule 1 to the Personal Data Privacy Ordinance (December 1996) by failing to take all reasonable practicable steps to ensure that personal data (the relevant "interest at stake," in that case) held by it was protected against unauthorized or accidental access, processing, erasure, or other use.[112]

Thus, this Article suggests that leaving devices security-wise unattended should be, today, a criminal offense to be prosecuted; subject to criteria of proportionality and reasonableness, this basic assumption should be included in criminal codes as to allow, as well, dual-criminality extradition procedures. The advice is to start outside the criminal sphere, possibly by means of soft laws at the international level (e.g. by

111. Barrat, *supra* note 55, at 244 (emphasis added).

112. Allan Chiang, *Reviewing the Personal Data (Privacy) Ordinance through Standstill and Crisis*, *in* Reforming Law Reform: Perspectives from Hong Kong and Beyond 207, 212 (Michael Tilbury et al. eds., 2014).

incorporating the concept into the next edition of the OECD Guidelines for Business Enterprises). It is also posited that public-funded organizations like the Asian Development Bank (ADB) should not receive those funds if the latter coalesce into development cooperation projects unable to protect their trade secrets. Supposedly, those trade secrets are meant to be a competitive advantage and support their corporate owners located in those beneficiary countries to grow. Developmentally speaking, there is little sense in publicly financing projects which show unwillingness to protect their most strategic assets; in other words, such a protection should feature in the project assessment sheets. Lastly, as the lightest form of "punishment," and as much as to endorse a trend of governmental accountability and open governmentality which finds the right to access *public* information to be a strategic ally,[113] states could publish a list of noncompliant companies ("naming and shaming"). The rationale would be that citizens have the right to know where collective money is spent as well as how and because of whom it goes wasted (needless to stress, this should be done whilst carefully keeping an eye on national security and *ordre public*). The right to access information is increasingly[114] understood as encompassing bilateral and multilateral arrangements to which the State is a party and/or involved member,[115] which echoes the point made above about the ADB, but might be stretched as far as to encompass state-participated multinational corporations in productive networks.

IV. Technical Aspects of Competitive Cyber Defense

Cyber-intrusions are firstly intrusions in a company's private sphere, i.e., in its privacy domain (if such a thing—corporate privacy—does exist). Over the last decades, "[d]octrines on copyright have been used to help ground a right to privacy, which has, in turn, helped ground data privacy law, while privacy doctrines have been used to help ground aspects of copyright."[116] Something similar occurred with competition law, although

113. Rio Declaration on Environment and Development, Principle 10.

114. This trend is confirmed by several scholarly writings. *See, e.g.*, Sanderijn Duquet & Jan Wouters, *Diplomacy, Secrecy and the Law*, *in* Secret Diplomacy: Concepts, Contexts and Cases 85, 97 (Corneliu Bjola & Stuart Murray eds., 2016) ("Unlike States, global international organizations do not commonly recognise a general right to information. However, a trend can be discerned towards more openness"). Nonetheless, the reasoning made above was referred to information held by States about those same States' political activities within the IOs, and not to information in possession of IO's Secretariats about IOs themselves in their "overall" bureaucratic configuration; these two may coincide but often time concern different categories of documents and acts.

115. *See, e.g.*, Principle 3 of the 2008 Atlanta Declaration and Plan of Action for the Advancement of The Right of Access to Information, the 2005 Right to Information Act in India, or Art.1(2)(b) of the 2009 Council of Europe's Convention on Access to Official Documents (not yet entered into force).

116. Lee A. Bygrave, Data Privacy Law: An International Perspective 13 (2014).

in this case what we are witnessing is just the beginning of a regulatory crossfertilization process. For instance, in Belgium, elements of data privacy law have infused traditional doctrines on "fair competition." In *AffCCH v. Generale de Banque* (1994) the plaintiffs (two federations of insurance agents) sued a bank for engaging in unfair competition occasioned by the bank's use of a particular strategy for marketing their services at the expense of similar services offered by the plaintiff. The sued bank analyzed data of its clients which they had acquired in the course of normal banking operations so it could offer the clients tailored financial services (insurances) that undercut the same services already offered by the plaintiff.[117] The judge made a finding not only of data privacy breach (finality principle), but also of doctrines of fair competition; arguably, in today's EU competition framework, this would stand as even truer. By any means, one should be cautious when transposing antitrust procedures into IP law (more than vice versa),[118] since:

> whereas [the former]'s remedial structure is heavy artillery that can chill innovation and competition, IP's remedial structure is more finely tuned to address complex problems of market power . . . . Ideally, however, antitrust, IP and other regulatory instruments should work conjunctively to make sure that the IP system grants just enough incentive for the creation of socially desirable innovations.[119]

Unauthorizedly acquiring (e.g. through cyberattacks) or disclosing (e.g. by reselling) trade secrets constitutes misappropriation. It can be performed by free hackers, criminal gangs, political "hacktivists," rogue employees, or foreign States.

> Although trade secret misappropriation occurring within the offended country and involving known offenders . . . can be redressed in civil litigation, the same is not true for cyber misappropriation that originates abroad. Of particular concern are the types of cases that involve unknown or anonymous offenders, who may or may not be in the attacked business' country of registration/incorporation, and who steal trade secrets through hacking . . . that involve remote access tools.[120]

When arms producers and other companies stand in between trade and security is involved, intelligence material may share the border with trade secrets, and economic value deriving from nondisclosure may match security concerns. Strategically,

> ICT firms [e.g. outsourcers of trade secret storages] are attractive to attackers, because they store large quantities of *valuable* data in

117. *Id.* at 15–16 n.66.

118. *See* Harry First, *Trade Secrets and Antitrust Law*, *in* The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research 332, 366 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011). This stands in accordance with Schumpeter's views.

119. Daniel A. Crane, *IP's Advantages over Antitrust*, *in* The Global Limits of Competition Law 117, 118–119 (D. Daniel Sokol & Ioannis Lianos eds., 2012).

120. Rowe, *supra* note 41, at 383.

> electronic form; [those firms] can also count on decision-makers who understand the threat, including that of data theft. These two factors combine to yield an intensive use of various protection systems.[121]

Technically, cyber defenses against intrusion, thefts, and espionage are classified as either active or passive: as in the West "[t]he failure of the government[s] to provide adequate protection has led many cybersecurity analysts, scholars, and policymakers to suggest that there is a need for private-sector self-help,"[122] companies should keep active defenses ready. At this point, the role of the State could be twofold: providing judicial "waiving" of legal hurdles arising from "reasonable" active defense, and placing the latter among the country's ordinary business laws as a requirement for companies. This way, not only the defensive cyber-hygiene, but also the offensive cyber-readiness would be legitimized and compelled, entering the common lexicon of corporate management as well as incident response.

> In 2010, a group from China allegedly hacked into Google's network and those of many other U.S. companies. Not only did Google successfully trace the source of the attack, but it also engaged in a counter-offensive move to obtain evidence about the culprits, in a sort of 'private self-help.' This has come to be known as 'hacking back,'[123]

which replicates the deterrent "second strike capabilities" model in the context of nuclear warfare[124] (the landmark difference being that the former is mostly left in the hands of uncontrollable private actors, whereas nuclear arsenals are firmly supervised by States). Besides municipal contexts, it is unclear whether "hacking back" is permissible under public international law: if anything goes wrong with the counterstrike, moves of attribution to the striker-hosting State for the sake of engaging its international responsibility are concrete and workable. The function and liability of intermediaries like the Internet Service Providers, which supply the ultimate access to Internet pages and products, are other "major challenge[s] for legal regimes related to digital copyright protection"[125] and remotely-stored trade secrets just as much. In this second case, they provide the platforms where trade secrets are released after having been thieved, although doing so is an economic suicide: trade secrets' value lies exactly in maintaining their secrecy even

121. Biancotti, *supra* note 55, at 10 (emphasis added).

122. Paul Rosenzweig et al., *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, Heritage Found. (May 5, 2017), https://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense [https://perma.cc/2DD9-35TN].

123. Rowe, *supra* note 41, at 418.

124. Peter Navarro, Crouching Tiger: What China's Militarism Means for the World 76 (2015) ("If I can strike your major cities back with a devastating salvo of nuclear missiles after you strike my cities first, you will be far less inclined to launch that first attack to begin with").

125. Ramaswamy Muruga Perumal, *Copyright Infringements in Cyberspace: The Need to Nurture International Legal Principles*, 14(3) Int'l J. Computer, the Internet and Mgmt 8, 16 (2006).

(. . . and *a fortiori*!) after having stolen them. There is in fact a debate on whether liability for cyber thefts should be allocated to the internet service providers as well, or exclusively to the alleged offenders.

V. A Fresh Public-Policy Approach yo Trade Secrets Theft

> One is tempted to . . . desire to see Law and Economics' institutional embeddedness (in the courts, in the law schools) shifted, if not displaced; its theorists (on the bench, at the podium) sidelined or demoted from their current positions of prominence; and the return of core jurisprudential values (of justice, of rights, of ethics) to a law released from the spell of "efficiency". And all that is required for this to come about is for a united front of "crits" to "out" Law and Economics as involving neither "the legal" (after all, *it reduces the law to its lowest common denominator, coercion*) nor "the economic" (owing to the limited and restricted nature of the economics it employs).[126]

Despite the provocative quote reported above, reproducing a controversy tracing back a long time,[127] we deem economic approaches to the law essential in policy and legal scholarship concerned with trade secrets. To begin with, there exists a debate on whether regulation should be "technology neutral" or tailored to the specific features of technologies;[128] in this case, on whether trade secret laws should be conceived (also) for the cyberspace as a specific *locus* of both protection and loss. Australia, for example, prompted the TRIPS Council to declare that the interpretation of the treaty's technologically-neutral rules should be explicitly readapted to digital environments, rather than rewriting those rules altogether.[129] Despite multiple benefits, the side effects of hypersecuritizing companies' cyberspace for the sake of protecting trade secrets cannot be overlooked. For example, "trade secrets law serves as a partial substitute for excessive investments in physical security";[130] as such, overprotecting cyber infrastructures may cause unsustainable

126. William P. MacNeil, Lex Populi: The jurisprudence of popular culture 94 (2007) (emphasis added).

127. *See, e.g.*, John H. Farrar & Anthony M. Dugdale, Introduction to Legal Method 267–268 (3d ed. 1990).

128. *See generally* Brad A. Greenberg, *Rethinking Technology Neutrality*, 100 Minn. L. Rev. 1495 (2016); Winston J. Maxwell & Marc Bourreau, *Technology Neutrality in Internet, Telecoms and Data Protection Regulation*, Hogan Lovells (2015), https://www.hoganlovells.com/en/publications/technology-neutrality-in-internet-telecoms-and-data-protection-regulation [https://perma.cc/L855-QXDC]. *See* Bert-Jaap Koops, *Should ICT Regulation Be Technology-Neutral?*, *in* Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners 77 (Bert-Jaap Koops et al. eds., 2006), for an earlier comment.

129. Submission from Australia, *Electronic Commerce Work Programme*, WTO Doc. IP/C/W/233 para. 5, 9–11 (Dec. 7, 2000).

130. Lorenzo de Martinis et al., *Study on Trade Secrets and Confidential Business Information in the Internal Market*, Eur. Union (Jul. 12, 2013), https://ec.europa.eu/growth/content/study-trade-secrets-and-confidential-business-information-internal-market-0_en [https://perma.cc/3LGC-K2EY].

money-spending financial commitment, making the very choice for trade secrets no longer convenient. Cost-efficiency is a particularly important variable in the preference for trade secrets, as to counterbalance one of their worst downsides: as they "encourage an excessively proprietary approach and the creation of barriers resulting in market inefficiency,"[131] they are a worthy choice in macroscopic terms only as far as they are able to streamline a country's productive-entrepreneurial system. "Requiring innovators to take reasonable precautions to insure the secrecy of their innovations forces innovators to focus efforts on precautions as opposed to innovations."[132] Having due regard for the above, one may conclude that from a public perspective, state-mandated (or even state-funded) hypersecuritization of corporate IT networks is certainly convenient when attempts of international theft are reasonably expected, and only moderately convenient when it comes to domestic thefts. Indeed, the following scenarios can be introduced.

Let us suppose that A and B are two companies registered in the same country, and B steals a trade secret from A; A cannot rely on this competitive advantage anymore, but B cannot do it either, as the trade secret is only valuable insofar it is known to an economic actor only, within the same *relevant market*. The consequence is that neither A nor B can work alone anymore, therefore they will likely merge or at least establish a joint line of products and/or services reliant on the stolen trade secret. This simplified scenario illustrates that, independently from A's recourse to compensational justice, and leaving the negligible oligopolistic practices a joint A-B venture would give rise to aside, a stolen trade secret remains somehow "useful" within the borders of a domestic economy. Needless to say, this does not hold true internationally, as the country which steals the secret enjoys all incentives to escape compensational justice, to not cooperate business-wise, and to develop technologies capable of more proficiently exploiting industrially the stolen secret. These scenarios help qualify the assumption that "systemic issues related to technology . . . will continue to make legislative and judicial solutions suboptimal for cyber misappropriation":[133] it *depends*. Whereas the pursuance of judicial remedies (offenders' identification and prosecution; monetary and nonmonetary compensation) to trade secret theft—which has regrettably been the focus of the whole legal scholarship[134] on trade secrets to date—is to be considered obsolete, ineffective and unfruitful, legislative measures can prove useful, as long as they focus on cyber-hygiene and cyber-readiness rather than on traditional, unserviceable legal approaches. The perspective is not banally of self-defense on the

131. *Id.*

132. Jon Chally, *The Law of Trade Secrets: Toward a More Efficient Approach*, 57 VAND. L. REV. 1269, 1307 (2004).

133. Rowe, *supra* note 41, at 392.

134. With a few exceptions in gray literature, such as in think-tank reports or policy briefs drafted by multinational consultancy firms.

faction of trade secret owners;[135] rather, emphasis is placed on legislative measures targeting the only actors able to solve trade secret thefts' root-causes: those who hold such IP in the first place. Propositions such as the one that "a competitor's actions should constitute misappropriation [only] if an innovator, to maintain the secrecy of her information, would have taken precautions to the level that the benefit achieved from any further precautions would be outweighed by the costs of implementing such precautions"[136] are to be considered economically meaningful for single cases, yet politically and industrially untenable from a public perspective when it comes to systemic risks to a country's security assets and innovation capabilities. Beyond the domestic sphere, the cost-effectiveness of trade secret protection should be complemented by additional policy considerations.

A. *The Shortcomings of Post-Factum Judicial Intervention*

Trade secrets' low entry-cost is appealing to SMEs, but *exactly because* there is no bureaucratic procedure *a priori* protecting trade secrets (i.e., overtly recognising them as such, e.g. in a public registry), and so once stolen they can be used to whatever end, one must rather act on preventing the misappropriation from happening. A company can be damaged by either the disclosure of a trade secret to its competitors, or by the reselling of the trade secret to foreign powers. On this, one shall note that "[i]f a purchaser buys a product that contains a trade secret, like . . . an electronic product containing secret software code, the mere act of reselling the product does not entail misappropriation. The right to resell . . . does not arise from exhaustion of the trade secret right."[137] Overarchingly, it is true that court injunctions may prevent disclosure of trade secrets and preserve evidence, but such injunctions are de facto impossible to enforce extraterritorially; thus, when international violations occur, the damage to the country's economy and to the social body (especially that of taxpayers' citizens) persists. As it is often the case that foreign countries do not cooperate in these sort of investigations "due to their own weak response," seizing probative-enough evidence abroad proves almost impossible.[138] Therefore, we strongly rebut the "arguments" of those[139] who claim that misappropriations from unknown, external-to-a-company agents should not be a great concern just because they do not represent a majority of court cases: if they do not, it is because courts

135. *See, e.g.*, *id.* at 383.

136. Chally, *supra* note 132, at 1306.

137. Shubha Ghosh & Irene Calboli, Exhausting Intellectual Property Rights: A Comparative Law and Policy Analysis 188 (2018).

138. Melanie Reid, *A Comparative Approach to Economic Espionage: Is any Nation Effectively Dealing with This Global Threat?*, 70 U. of Miami L. Rev. 757, 802 (2016).

139. *See, e.g.*, David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291, 303–304 (2010).

can notoriously do little about them, especially internationally.[140] Court injunctions are important nationwide, though: e.g. in Japan,

> [t]he Unfair Competition Prevention Act (Act No. 47 of 1993) prohibits certain acts (unfair competition), including an act to acquire a trade secret from the holder by theft, fraud or other wrongful methods; and an act to use or disclose the trade secret so acquired. For the prevention of unfair competition, the Act provides measures, such as *injunctions*, claims for damages and penal provisions.[141]

In the United States,

> [the] Defend Trade Secrets Act (DTSA) also provides federal legislative protection for information by expanding access to judicial redress for unauthorised access and use of trade secrets. [It] . . . authorises a federal court to grant an injunction to prevent actual or threatened misappropriation of trade secrets, but the injunction may not prevent a person from entering into an employment relationship; nor place conditions on employment based merely on information the person knows . . . . Moreover, the DTSA precludes the court from issuing an injunction that would 'otherwise conflict with an applicable state law prohibiting restraints on . . . business.'[142]

Not even the much more innovative *ex parte* seizure order[143] seems to be solving much. First, the evidentiary threshold for its enactment is

140. David Orozco, *Amending the Economic Espionage Act to Require the Disclosure of National Security-Related Technology Thefts*, 62 Cath. U. L. Rev. 877, 894 (2014) ("Despite the difficulty in addressing trade secret theft, civil litigation of *domestic* trade theft is on the rise, demonstrating the importance of trade secret information. However, this increase reflects only *domestic* civil suits, not claims brought under the EEA") (emphasis added).

141. Tomoki Ishiara, *Japan*, *in* The Privacy, Data Protection and Cybersecurity Law Review 220, 232 n.70 (Alan Charles Raul ed., 5th ed. 2018). *See also* Masao Yanaga, Cyber Law in Japan 118 (3d ed. 2017).

142. Alan Charles Raul & Vivek K. Mohan, *United States*, *in* The Privacy, Data Protection and Cybersecurity Law Review 376, 383 (Alan Charles Raul ed., 5th ed. 2018).

143. *See* Jonathan E. Schulz, Ex Parte *Seizure Orders under the Defend Trade Secrets Act: Guidance from the Courts during the Statute's First Year*, Bradley (Jun. 26, 2017), https://www.bradley.com/insights/publications/2017/06/ex-parte-seizure-orders-under-the-defend-trade-secrets-act-guidance-from-the-courts [https://perma.cc/C6FK-GX6J]; Timothy Lau, *Trade Secret Seizure Best Practices Under the Defend Trade Secrets Act of 2016*, Fed. Jud. Ctr. (Jun. 2017), https://www.fjc.gov/sites/default/files/2017/DTSA_Best_Practices_FJC_June_2017.pdf [https://perma.cc/6Y3Z-X5WT]; Kevin Burns, *The DTSA's* Ex Parte *Seizure Remedy—Two Years Later*, Fisher Phillips (Aug. 7, 2018), https://www.fisherphillips.com/Non-Compete-and-Trade-Secrets/DTSA-ex-parte-seizure-remedy-two-years-later [https://perma.cc/MLL9-5NS4]; Ali Dhanani, *The New Defend Trade Secrets Act: Finally, A Federal Tool to Protect Your Trade Secrets*, Baker Botts (Jul. 2016), http://www.bakerbotts.com/insights/publications/2016/07/ip-report-a-dhanani [https://perma.cc/7KLN-AMM5].

very high (and rightly so).[144] Secondly, there is the fear of trolls[145] and "anticompetitive litigation with businesses attempting to seize their competitor's trade secrets".[146] Third, it will be made recourse too infrequently due to trade secret owners' liability if their request is found excessive.[147] Fourth, and most relevant for the present discussion, because secrets, by definition, cease to be so when someone unwanted gains access to them, and civil seizures are only capable of "prevent[ing] propagation or dissemination"[148] once the harm has already occurred. The true fact that the secret is visualized, heard, or memorized may hinder its IP-protective and competitive function, independently from its eventual use by the criminals. This remark also explains the low rate of lawsuits as the violated owners' fear that their trade secrets will be exposed (and thereby lost) during the course of civil and criminal proceedings;[149] this stands even truer in common-law systems where adversarial trials are the norm, for the evidence is not sought by the judge directly but accessed and challenged by the parties themselves. Only certain arbitration fora may prevent this procedural exposure from happening,[150] but they could prove unaffordable for most startups. If arbitration allows for this improvement, it is no surprise that bilateral investment treaties (BITs) are more and more the *locus* of cybersecurity provisions encompassing the theft of trade secrets;[151] to be noted, scholarly literature has already explored

144. Remarkably, the amended Art.32 of China's Law Against Unfair Competition "reverses the burden of proof in civil trade secret suits when the plaintiff makes certain prima facie showings." Melissa Cyrill, *China Reinforces IP Laws to Protect Trademarks, Trade Secrets*, China Briefing (Apr. 25, 2019), https://www.china-briefing.com/news/china-ip-protections-trademarks-trade-secrets [https://perma.cc/26MU-QA77].

145. Follow the rebuttal of this fear in Joseph Brees, *Trade Secrets Go Federal—Parade to Follow*, 12 J. Bus. & Tech. L. 277 (2017).

146. Brittany S. Bruns, *Criticism of the Defend Trade Secrets Act of 2016: Failure to Preempt*, 32 Berkeley Tech. L.J. 469, 486 (2018).

147. Steven E. Holtshouser & Bryan K. Wheelock, *Can You Keep a Secret? Protection of Trade Secrets in Missouri*, St. Louis B. J. 34, 39 (2017).

148. Dobrusin, *supra* note 28, at 319.

149. Rowe, *supra* note 41, at 389; Mark Schultz et al., *Using IP Best Practices Dialogues to Improve IP Systems Globally: The Example of the Trade Secrets Law Best Practices Dialogue*, 26 George Mason L. Rev. 88, 93 (2018).

150. Draft Cybersecurity Protocol for International Arbitration, Int'l Council Com. Arb. 1, https://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf ("International arbitration in the digital landscape warrants consideration of what constitutes reasonable cybersecurity measures to protect the information exchanged during the process. Recognizing this need, the International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention and Resolution (CPR) and the New York City Bar Association have established a Working Group on Cybersecurity in Arbitration[, which] has promulgated a Draft Cybersecurity Protocol for International Arbitration proffered for public consultation. The consultative period [lasted] until 31 December 2018"). Such Draft Protocol lists "trade secrets" among the "types of confidential commercial information and/or personal data that may require special care." *Id.* at 12.

151. Onyema Awa Onyeani, The Obligation of Host States to Accord the

the possibility to accommodate investors' digital assets characterizable as trade secrets within the protective purview of the in-itself-debated BITs' "full protection and security" standard.[152] "[A] host [S]tate's fulfilment of its FPS commitment in a treaty instrument may involve security undertakings that are beyond its economic capacity, especially in the case of Developing States, where many so-called 'cyber attacks' are believed to originate."[153]

The above concurs to shape the impression that approaching trade secret thefts as a "property" or "freedom of speech" issue fails to do justice to businesses' efforts—especially the most vulnerable among them—to protect their key information. A self-explanatory example comes with the republication of stolen trade secrets, which is often pardoned by courts[154] via recourse to a "human rights-fashioned" language which seems inappropriate in this context (except for cases when such trade secrets may seriously violate an individual's dignity or privacy). Empirical studies[155] have conceded that the priority credited by leaving employees to sociomoral norms rather than legal ones when (and if) they decide not to carry trade secrets with them from the former employer to the next one, is a consequence *and not the cause* of the lack of credible enforcement mechanisms and convenient judicial remedies in trade secrets law. Judicial ineffectiveness prompts the need for higher state

---

Standard of "Full Protection and Security" to Foreign Investments Under International Investment Law 234 (Jan. 2018) (unpublished Ph.D. thesis, Brunel University London) (on file with Department of Law Brunel University London).

152. *See* David Collins, *Applying the Full Protection and Security Standard of International Investment Law to Digital Assets*, 12 J. World Inv. & Trade 225, 226 (2011) ("[t]he BIT between Argentina and the United States includes the expansive phrase: 'inventions in all fields of human endeavor' and '*confidential* business information' in its definition of intellectual property") (emphasis added).

153. *Id.* at 225. Indeed, in this case as well, the losing State would make the whole society pay; for these reasons, the financial burden should shift onto companies which did not comply with regulation put in place by the State in due time, subject to reasonable expenditure demands. However, there is a particular issue at stake in arbitration cases, which will be just mentioned *en passant* here as it falls beyond the scope of this contribution. The issue is that for the host State to regulate (or at least "indirectly oversee") the internal cybersecurity policies of companies which are registered or do substantial business within its territory, those companies must be nationals of that States? Incorporated companies are usually so, but this is not obvious, and the complex nationality assessment is to be performed on a case-by-case basis by the arbitrator concerned, following precedents, customs, and doctrines. The last relevant point is that if a State does not timely legislate on minimum cyber-hygiene standards for the companies registered therein, and one of the latter, by being breached, causes loss of assets/money/etc. to a foreign investor (either individual or legal person), that State negligently disattends its duties under the BIT protecting that foreign investor.

154. Jon L. Mills & Kelsey D. Harclerode, *Privacy, Mass Intrusion and the Modern Data Breach*, 69 Fla. L. Rev. 771, 815–816 (2017).

155. *See, e.g.*, Yuval Feldman, *The Expressive Function of Trade Secret Law: Legality, Cost, Intrinsic Motivation, and Consensus*, 6 J. Empirical Legal Stud. 177, 203 (2009), discussing a "classic" study, tailored to the Silicon Valley.

legislative interventionism,[156] aimed at reinforcing companies' self-responsibilization; judges themselves, for decades, have consistently referred to commercial ethics in their judgements,[157] arguably because they find themselves on the edge between unhelpful laws to be applied.

By way of summary, judicial measures are still important for building a doctrine,[158] but they usually come too late, too narrow in interpretative scope,[159] enforcement reach, *ratione loci* and *ratione materiae*,[160] as well as too exception-filled,[161] unpredictable (when not arbitrary),[162]

156. Andrei Shleifer, *Understanding Regulation*, 11 Eur. Fin. Mgmt. 439, 441 (2005) ("With well-functioning courts enforcing property rights . . . , the scope for desirable regulation—even by a "helping hand" government—is minimal"). However, later in the same paper, how this might slightly differ depending on the jurisdiction concerned (civil/common law, developed/developing economy, litigiousness rate, etc.).

157. Don Wiesner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 Md. L. Rev. 1076, 1077 (1988) ("[C]ourts believe that ethical standards are of some assistance in applying trade secret principles, particularly in cases of first impression").

158. *See, e.g.*, Villasenor, *supra* note 56, at 340 (in the US, the Federal Circuit finds that the Economic Espionage Act applied "even though misappropriation occurred outside the United States, because the subsequent importation would lead to unfair competition").

159. The landmark case in this respect is *U.S. v Nosal*, where "shortly after leaving an executive search firm, a former employee convinced former colleagues who were still working for the firm to help him start a competing business. . . . The accomplices used their log-ins to download client information and send it to the defendant in violation of a policy prohibiting the disclosure of confidential information . . . . The Ninth Circuit held that these activities did not constitute a violation of the CFAA because the accomplices were authorized to access the information, even if their subsequent use of the information violated the employer's policies." Jeffrey S. Klein et al., *Access v. Use: The CFAA in the Age of the DTSA*, Weil (Feb. 2018), https://www.weil.com/articles/access-v-use-the-cfaa-in-the-age-of-the-dtsa [https://perma.cc/W5ZC-A2F2].

160. *See, e.g.*, Salvucci, *supra* note 46, at 189.

161. *See, e.g.*, Robert Damion Jurrens, *Fool Me Once:* U.S. v. Aleynikov *and the Theft of Trade Secrets Clarification Act of 2012*, 28(4) Berkeley Tech. L.J. 833 (2013). Later on the same case, see Brendan Pierson, *Ex-Goldman programmer Aleynikov wins dismissal of second conviction*, Reuters (Jul. 6, 2015), https://www.reuters.com/article/us-goldman-sachs-aleynikov-appeal-idUSKCN0PG1L020150706 [https://perma.cc/F9Q6-ZNG6].

162. *See, e.g.*, this comment on the United States's case law: "In *Servomation Mathias, Inc. v. Englert*, the court held that lapses in the company's security program—through no direct fault of its own—would have made it very difficult for the company to prevail on the ultimate merits of its claim and, therefore, denied a request for a preliminary injunction. On the other hand, computer systems that are password protected are sometimes, but not always, held to be reasonable secrecy precautions sufficient to protect the trade secret. For example, in *Superchips Inc. v. Street & Performance Electronics Inc.*, both password protection and encryption of the key data were required for the court to find that reasonable secrecy precautions had been taken. And in *A.M. Skier Agency, Inc. v. Gold*, the court concluded that merely password protecting data in a computer was strong evidence that the plaintiff had taken reasonable secrecy precautions in order to protect the trade secret. In contrast, in *Softchoice Corp. v. MacKenzie*, information that was held under lock and key and password protected when stored on computers was not held to be the subject of reasonable secrecy precautions. And in *Southwest Stainless, LP v. Sappington*, even though the employer did password protect its trade secret among other secrecy precautions, other conduct

and burdened with evidentiary challenges[163] (including the required level of detail for alleging a misappropriation, and discovery requests by the alleged misappropriator[164]). Further, restrictions *ratione personae* make it difficult for judges to charge with misappropriation when the actual thief is unknown and a third party is simply taking advantage of the former's misconduct; this provides ill-intentioned third parties with a strong "incentive to seek out bad actors such as disgruntled employees[,] to misappropriate trade secrets for them."[165] Moreover, judges who are loyal to the springboard doctrine grant injunctions limited in time, claiming (often without substantiating their claims) that the harm in disclosing confidential information only occurs when executed within a certain period.[166] Evidentiary limitations pair with all the hurdles already outlined, for instance when an employer discovers a trade secret theft and rushes to collect evidence by disregarding the employer's data protection rights: depending on the jurisdiction, evidence so collected might help the alleged misappropriator evade liability rather than nailing them.[167] In sum, judicial remedies formulated in trade secret laws, to date and generally across jurisdictions, are in fact *not* tailored to the specificity of trade secrets: rather than protecting them by framing them *also* in security terms, they simply replicate the protection patterns elaborated for other IP rights, and built on the paradigms of either "property" or "liability".[168]

As the uncertain ROI of startups (especially those at seed stage, still testing their products' beta-version) can act as a deterrent to higher cybersecurity measures, States should contribute to startups' cybersecurity costs, provided that these companies have the right management and ambition in place to effectively manage their IT systems and drive the innovation locomotive; related antitrust concerns should be sharply dismissed: one can hardly associate these security subsidies with "state aid." Capitalism is widely acknowledged to represent a failure in itself, and yet still a tremendous opportunity when accurately corrected and overseen by national and global institutions.[169] If Keynes was right in affirming that increased state expenditure is more beneficial to state economy than

by the employer was sufficient to defeat its trade secret protection."). Trygve Meade, *Indecision: The Need To Reform The Reasonable Secrecy Precautions Requirement Under Trade Secret Law*, 37 S. Ill. U. L.J. 717, 726 (2013).

163. Just as an exemplification, *see* United States v. Dongfan "Greg" Chung, 659 F.3d 815 (9th Cir. 2011). *See also* Bently, *supra* note 11 at 1143–1144.

164. On the latter, *see generally* Jayme A. Sy Jr. and Jason L. Sy, *Discovery of Trade Secrets: A Procedural Quagmire*, 62(4) Ateneo L.J. 1218 (2018).

165. Jonathan R. K. Stroud, *The Tragedy of the Commons: A Hybrid Approach to Trade Secret Legal Theory*, 12(2) Chicago-Kent J. of Intell. Prop. 232, 241 (2013).

166. Bently, *supra* note 11 at 1150–1151.

167. Determann, *supra* note 19, at 134–135.

168. For a reference to patent protection conceptualizing patent infringement under property rules or liability rules, *see* Thomas F. Cotter, Comparative Patent Remedies: A legal and economic analysis 53 (2013)..

169. Nico Stehr and Reiner Grundmann, The Power of Scientific Knowledge: From Research to Public Policy 38 (2012).

prolonged high unemployment rates,[170] then the state capitalization of cybersecurity programs is to be preferred over the unemployment consequent to lack of faith on the part of entrepreneurs and investors that the trade secrets they coined and/or own will be safely protected against international competitors. This is true only as far as international contexts are concerned, since in a domestically closed economic circle the default of a company due to trade secret theft is compensated by the advantage the other domestic competitors gain out of the new possession of that secret. Resultantly, the national or international dimension of the (expected) theft does play a role; two considerations must be made, though: first, it is hard to predict (technically and geopolitically) whether attacks will come from nearby or abroad, and second, goods and services' markets are increasingly globalized and integrated within transnational exchange mechanisms. The globalization of IP threats and opportunities responds to the "primary rationalization of the demands of market actors pursuing maximum returns for innovative products in the global market."[171]

B. *The Consequences of Trade Secrets' Stealing Domestically*

Given that both our information society[172] and global economy[173] are built on intellectual property rights and on massive political bargaining over the governance thereof,[174] there is probably no need to stress the importance of information-based innovation today, nor to (legally) define it; yet, it is only with later scholarly adaptations of Schumpeter's work that the nexus between innovation, development, knowledge, entrepreneurship and IP rights has been unearthed and analyzed through hybrid legal-economic studies.[175] From a Schumpeterian perspective, immaterial assets made of intellectual property are forms of capital providing controlling power over production processes;[176] the nonabstract ones are capital (thus can be traded) by definition. This might sound rather intuitive today, but it was not doctrinally banal before his work, and carries noteworthy implications for our examination. The true revolution operated by Schumpeter was to replace price competition with knowledge-based, innovation-imitation models as the core playing paradigms

170. *Id.* at 36–37.

171. Ruth Lade Okediji, *The International Relations of Intellectual Property: Narratives of Developing Country Participation in the Global Intellectual Property System*, 7 Sing. J. of Int'l and Comp. L. 315, 365 (2003).

172. Megan M. Carpenter, *Intellectual property: A human (not corporate) right*, *in* The Challenge of Human Rights: Past, Present, and Future 326 (David Keane et al., eds., 2012).

173. Harry Williams Arthurs, (2001) *The re-constitution of the public domain*, *in* The market or the Public Domain? Global Governance and the Asymmetry of Power 97 (Daniel Drache ed., 2001).

174. *See generally* Sebastian Haunss, Conflicts in the Knowledge Society: The Contentious Politics of Intellectual Property 11–94 (2013).

175. Rami M. Olwan, Intellectual Property and Development: Theory and Practice 115 (2013).

176. Peter Drahos, A Philosophy of Intellectual Property 156–157 (1996).

for successful corporations (and thus, overall technological progress) in capitalist markets;[177] resultantly, "it is not dynamic efficiency which [the] law should directly be aiming at[,] but the maintenance of market structures which favour creativity."[178] Equilibrium is displaced by a series of temporary monopolies which "are common, but frequently swept aside by new ones."[179] For example, the Schumpeterian model of entrepreneurial competition may offer essential insights to reflect upon:

> [W]hen it is successful and therefore profitable, innovation induces other covetous of the innovational rents to imitate the actions of entrepreneurs, either by simple duplication or by producing substitutes. In the process, the imitators increase the demand for labor, capital, and other factors of production, thus pushing up their prices and the entire schedule of average costs. By increasing the supply of goods and services, they push down their prices. The increase in unit costs and the fall in supply prices eventually eliminate the rents of entrepreneurship and bring forth the circular flow equilibrium of neoclassical theory. The innovators or entrepreneurs of Schumpeter's model are . . . temporary monopolists[, since] their actions cause changes in the quality of market structure and entrepreneurial power.[180]

Trusting this theory, one can conclude that when a trade secret is stolen domestically, that asset simply flows back into the same economy by fuelling the "imitating attitude" of other entrepreneurs whom, once recovered from the time disadvantage and adaptation gap from the previous owner, will end up replacing the original products and/or services offered by the violated company through the possession and usage of that secret. Beyond macroeconomic neutrality, this might even turn out positive, as to circumvent the rents levelling stressed before, facilitate interoperability,[181] and catalyze improvement. Informal local networks of know-how sharing should be encouraged.[182] After all, patents and trade secrets lie at the foundation of most Schumpeterian "creative destructions" that keep capitalism going;[183] those disruptive gestures can

177. Wolfgang Kerber, *Competition, innovation and maintaining diversity through competition law*, *in* Competition Policy and the Economic Approach: Foundations and Limitations 175–176 (Josef Drexl et al. eds., 2011).

178. Andreas Heinemann, *The impact of innovation—comments on Uwe Cantner and Wolfgang Kerber*, *in* Competition Policy and the Economic Approach: Foundations and Limitations 211 (Josef Drexl et al. eds., 2011).

179. Ariel Katz, *Making Sense of Nonsense: Intellectual Property, Antitrust, And Market Power*, 49(4) Arizona L. Rev. 837, 874 (2007).

180. Albert Breton, Competitive Governments: An Economic Theory of Politics and Public Finance 32 (1998) (one in-citation emphasis removed).

181. Gustavo Ghidini & Emanuela Arezzo, *One, none, or a hundred thousand: How many layers of protection for software innovations?*, *in* Research Handbook on Intellectual Property and Competition Law 363–364 (Josef Drexl ed., 2008).

182. *See generally* Laura G. Pedraza-Fariña, *Spill Your (Trade) Secrets: Knowledge Networks as Innovation Drivers*, 92(4) Notre Dame L. Rev. 1561 (2017).

183. David H. Gobell, Harold F. Koenig, and Chandra S. Mishra, *Strategic Value Creation*, *in* Technological Entrepreneurship 8 (Phillip H. Phan ed., 2002).

be cooperative outcomes among multiple businesses, yet only insofar as such cooperation comes as a "mishap" and originated in competition.[184]

Performed through political economy lenses, the above-mentioned theory considers *stolen* trade secrets as a form of disclosed—thus widely exploitable—knowledge capable of spillover effects from micro to macro industrial productions and of socializing implicit norms of behavior within a closed entrepreneurial system (like the entrepreneurial texture of a country can be deemed to be, for the sake of this discussion). "By reducing risk, trade secret law promotes the sharing of trade secrets with a broader circle of contacts, which may lead to follow on innovation and greater development of human capital."[185] The so-called "knowledge spillover theory of entrepreneurship"[186] reads the latter as an "endogenous response to the incomplete commercialisation of new knowledge,"[187] i.e., to investments in knowledge that are not fully appropriated by incumbent firms.[188] SMEs are deemed able to generate innovative outputs while spending little in R&D, through the exploitation of knowledge by higher expenditures on research in universities and R&D in large corporations. Put differently, knowledge (research), which is "nonexcludable and nonrival in use,"[189] triggers low-cost innovation. An impoverishment in either side—SMEs or big companies—impoverishes the other insofar as investment in knowledge is triggered by spatial proximity to the knowledge source, in a sort of "innovation district" whose major members' spill over effect is exploited by the smallest companies. Whilst traditional economic theories used to suggest that small firms retard economic growth, contemporary theories of industrial evolution suggest that diffused entrepreneurship will stimulate and generate

184. Breton, *supra* note 180, at 33.

185. Douglas C. Lippoldt, & Mark F. Schultz, *Trade Secrets, Innovation and the WTO*, E15 Expert Group on Trade and Innovation 2 (2014), http://e15initiative.org/wp-content/uploads/2015/09/E15-Innovation-LippoldtSchultz-FINAL.pdf [https://perma.cc/Q8G4-NL42].

186. *See generally* Zoltan J. Acs, Pontus Braunerhielm, David Bruce Audretsch, and Bo Carlsson, *The knowledge spillover theory of entrepreneurship*, 32(1) Small Bus. Econ. 15 (2009).

187. David Bruce Audretsch, Max C. Keilbach, and Erik E. Lehmann, Entrepreneurship and Economic Growth 35 (2006).

188. David Bruce Audretsch & T. Taylor Aldridge, *Knowledge spillovers, entrepreneurship and regional development*, *in* Handbook of Regional Growth and Development Theories 201 (Roberta Capello and Peter Nijkamp eds., 2010). *See also* Maria Cristina Cinici & Daniela Baglieri, *(Not) energizing microelectronics ecosystems through a large firm's inventor network: Lessons from Italy*, *in* Entrepreneurship and Talent Management from a Global Perspective: Global Returnees 232 (Huiyao Wang & Yipeng Liu eds., 2016) ("For example, when securing a patent, a firm produces new knowledge and the information included in the patent becomes accessible to the general public and competitors. In fact, knowledge-generating firms run the risk of not fully appropriating or internalizing the returns on knowledge investments, and some returns spillover to benefit others as well.").

189. Prashanth Mahagaonkar, Money and Ideas: Four Studies on Finance, Innovation and the Business Life Cycle 15 (2009).

growth, as part of the just-mentioned virtuous cycle with the major counterparts. As new-Schumpeter hypotheses based on recent empirical findings suggest that the concentration variable is only one (and a *minor* one) of the several factors impacting variance in R&D intensity,[190] sector-specific technological opportunity in the form of technical knowledge and entrepreneurial know-how (trade secrets) influences innovation more evidently.[191]

This Subpart can be summarized by observing that in a domestic theft of trade secrets, two phenomena offset each other: an enhanced (positive) competition stemming from the disruption of the secret owner's information monopoly, and the (negative) disincentive to invent on the part of the stealer.[192] Considering also the time and monetary resources spent to actualize this transaction—or transfer—by both sides, one may conclude that domestic thefts of trade secrets are macroeconomically neutral, or under certain conditions, *slightly* beneficial or detrimental to the economy of a country depending on the market structure and transaction costs. So far so good (but it must be kept in mind that the perspective offered in this Article is exclusively the public, "common good" one); the implications of trade secret thefts worsen when *international* breaches are involved.

C. *The Consequences of Trade Secrets' Stealing Internationally*

> *The protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation . . .* [193]

The preceding paragraphs have succinctly interpreted the outcome of an intra-system stealing, by suggesting what added value trade secrets—from a public policy perspective—would equip societies with; in other words, it has answered the question: "what happens if trade secrets are stolen within a country?". The finding was influenced by the proposition that although trade secrets fuel innovation and incentivize improvement,[194] "firms' abilities to combine first-mover advantages with trade secrets . . . may afford them secure long-lasting monopolistic positions despite their low rate of (radical) innovations and not because of it. The outcome is . . . the danger of replacing Schumpeterian profits with rent extraction and Schumpeterian competition with zero-sum

190. Uwe Cantner, *Industrial dynamics and evolution—the role of innovation, competences and learning*, *in* Competition Policy and the Economic Approach: Foundations and Limitations 151–152 (Josef Drexl et al., eds., 2011).

191. Bruno Crépon, Emmanuel Duguet, and Isabelle Kabla-Langlois, *Schumpeterian Conjectures: A Moderate Support from Various Innovation Measures*, *in* Determinants of Innovation: The Message from New Indicators, (Alfred Kleinknecht ed., 1996).

192. David D. Friedman, William M. Landes, and Richard Allen Posner, *Some Economics of Trade Secret Law*, 5(1) J. of Econ. Persp. 61, 69–70 (1991).

193. TRIPS Agreement, *supra* note 7, at Art. 7.

194. Leonardo Burlamaqui, *Knowledge governance, innovation and development*, 30(4) Brazilian J. of Pol. Econ. 560, 563 (2010).

game exclusionary practices."[195] As such, *exclusively in public and macroeconomic terms*, the theft of trade secrets in closed national systems was deemed not problematic, standing at worst as neutral, and at best as even slightly beneficial to the entrepreneurial, innovative vitality of those systems by abating their "information feudalism" that privileges the few over the masses.[196]

It is now time to turn to hint at a possible investigation of the potential consequences of an extra-system theft of trade secrets, thus answering the reverse question of what happens when they are stolen by external competitors in potentially open systems and *not* by intra-system competitors. The aforementioned "entrepreneurial incentive" is one of the parameters used by U.S. courts to evaluate redress in misappropriation of trade secret cases.[197] Such an incentive equates to "the amount of economic benefit required to motivate the intangible asset creator to enter into the development process[, and] is often perceived as an opportunity cost."[198] My reconceptualization theorizes the existence of a *nationwide* "entrepreneurial incentive" as well: a State—or its overall entrepreneurial network—innovates when the expected return is worth it. In the case under scrutiny here, this means that a State innovates through trade secrets only when there are reasonable expectations as for the security of those intangible assets, their chain of custody, and risk management policies related thereto. Put differently, a State opts for seeking assurances those trade secrets will not get stolen, especially by foreign competitors; this thieving activity—particularly when repeated over time and/or on a massive scale—would disrupt the competitiveness of the whole economic system of the State concerned. Once a trade secret is stolen, it—and at times, the company owning it—cannot be sold at even a strikingly low price, which stands as one of the clearest differences between this and other kinds of intellectual property. Adopting reasonable measures to protect their trade secrets in time is up to the companies themselves, *and so should be their liability* for negligent noncompliance: What shall be avoided is a burden shift on individuals and societies. Obviously, eventual deductions under the corporate tax laws are to be disallowed for incompliant companies, and any sort of production incentive discontinued.

195. Leonardo Burlamaqui, *Knowledge Governance: An Analytical Approach and its Policy Implications*, *in* Knowledge Governance: Reasserting the Public Interest 10 (Leonardo Burlamaqui et al., eds., 2014).

196. Burlamaqui, *supra* note 195, at 567.

197. Shawn D. Fox, *Calculating Damages in Misappropriation of Trade Secrets Matters*, Willamette Insights 21–22 (2016), http://www.willamette.com/insights_journal/16/spring_2016_2.pdf.

198. Robert F. Reilly, and Robert P. Schweihs, Guide to Intangible Asset Valuation 225 (2016).

D. *Auditing, Tax Incentives and Burden-Shifting Avoidance*

> *[C]ybersecurity can function as a public good if its costs are shared equitably among the relevant stakeholders. . . . But managing cybersecurity as a public good would also yield three important advantages: systemic approaches to security, shared responsibilities among the different stakeholders, and fostering collaboration.*[199]

The traditional (yet challenged[200]) view holds that production decisions are essentially similar for firms under monopoly or monopolistic competition as they are for competitive firms: in either case, the firm maximizes its profits at a price-output level where its marginal costs equal marginal revenue.[201] The imposition of a corporation profit tax does not alter the profit-maximizing price-output combination in the short run; thus, firms under monopoly or monopolistic market structure also do not short-term shift taxes. However, firms may prioritize long-run profits (and the bigger firms are, the more they proceed this way), for which indeed a corporation profit tax may be deleterious; the state subsidiarization thereof may prevent firms from tax-shifting practices onto on the social body. If strategic assets like trade secrets are left exposed to even the most rudimental attacks, this value is dispersed and the State subsidiarization becomes not only a strategic failure in terms of public management, but also a financial loss shared among the taxpayers. The importance of these concepts emerges crystal-clearly in regard to the social cost of public startup investment funds, when one considers that the innovative texture of any economic system, and particularly its startup environment, need to be supposed in its longterm development plans. All the more so, during recession cycles, when the role of the State arguably widens.[202] With a legal mindset, it is necessary to specify—within the relevant policy documents—who is in charge of

199. Mariarosa Taddeo, Opinion, *To build trust, we could treat cybersecurity as a public good*, ITU News (Sep. 2, 2019), https://news.itu.int/15753–2 [https://perma.cc/X36Q-HEAE].

200. *See, e.g.*, Robert E. Hall, (1988) *The Relation between Price and Marginal Cost in U.S. Industry*, 96(5) J. of Pol. Econ. 921–947 (1988).

201. Richard George Lipsey, An introduction to positive economics 245–247 (4th ed. 1975); Mary Hall (2019) *How Is Profit Maximized in a Monopolistic Market?*, Investopedia (Apr. 2, 2019), https://www.investopedia.com/ask/answers/041315/how-profit-maximized-monopolistic-market.asp.

202. Maria Pinelli and Uschi Schreiber, *Funding the future: Access to finance for entrepreneurs in the G20*, EY 41 (2013) ("There is no question that the financial crisis and its aftermath have had a dramatic impact on the availability of funding, particularly in developed markets. Bank financing has declined, and equity funding has also waned as investors have become more risk-averse."). *See, e.g.*, Marie Ekelanda, Augustin Landierb, and Jean Tirolec, *Strengthening French Venture Capital*, 33 Notes du conseil d'analyse économique 1 (2016). *See also, e.g.*, James M. Boughton, Domenico Lombardi, and Anton Malkin, *The Limits of Global Economic Governance after the 2007–09 International Financial Crisis*, 8(4) Global Policy 30 (2017) (describing the 2008 financial crisis as "a turning point in the history of the post-war globalization experiment.").

determining when and under what circumstantial conditions the recessive phase justifies an expansive role of state subsidiarization of small innovative companies' cybersecurity expenditure, in order to preserve the national economic texture and its most fundamental (intangible) innovation assets. Summarizing, the State should subsidize corporate income tax as a form of indirect social-at-large contribution towards a service the whole community benefits from as well, i.e., protection of trade secrets and nonadvantaging practices in favor of foreign competitors. The scheme works straightforwardly with private companies. In the event of state-owned companies, considerations to be made are more complex.[203] Simply put, such a tax could be waived automatically when the shareholders are equally committed to the pursuance of cybersecurity enhancement,[204] considering that distributed profits could be taxed by subjecting them to personal income tax on shareholder dividends.

"[C]itizens see money they have paid over to government in a different way [than] money paid to a for-profit organisation. When a company declared large profits or losses only shareholders see the money as theirs, not every customer who has provided the turnover in the first place."[205] What citizens generally do not realize is that if they are all "*share*holders" of public money, they also are "*stake*holders" of the private one, or more accurately, of the relationship between public money and private money; they would better leverage on this position especially when the "public" invests (or otherwise tangibly counts) on the "private" and the latter fails in fulfilling its obligations (e.g. by not meeting the cybersecurity expectations placed upon it). Phrased otherwise, any private actor can produce public externalities (unforeseen effects on the public) in its relation to the public.[206] Citizens are "stakeholders" of publicly-funded privates as although they are not their beneficiaries or clients (output stakeholders), they help those privates to make business grow (input stakeholders).[207]

---

203. *See generally* Wei Cui, *Taxing State-Owned Enterprises: Understanding a Basic Institution of State Capitalism*, Osgoode Legal Studies Research Paper Series, No.124 (2016); *see also*, Wei Cui, *Taxation of State-Owned Enterprises: A Review of Empirical Evidence from China*, *in* Regulating the Visible Hand?: The Institutional Implications of Chinese State Capitalism 109–132 (Benjamin L. Liebman and Curtis J. Milhaupt eds., 2015).

204. Some U.S. cities have proposed experiments in this direction, as a reward for environmental compliance or overpositive performance. *See* Kristen Jeffers, *How corporate tax incentives work and why cities spend so much on them*, Greater Greater Washington (Jun. 26, 2018), https://ggwash.org/view/68136/heres-how-corporate-tax-incentives-work-and-why-cities-give-them [https://perma.cc/RZG9-LVEF].

205. Gary Bandy, Financial Management and Accounting in the Public Sector 5 (2014).

206. Perhaps a classic example of externality could be the water pollution emanating from a factory producing certain goods onshore a river: in a completely free market, the factory owners would not have any incentive to spend money on technology to protect the environment, nor would they bear the costs to clean up the polluting effects; in practice, governments have implemented regulatory systems requiring factories to reduce their pollution, by intervening in the market equilibria.

207. This stands as a reformulation of and adaptation from the public management

Of course this description falls trapped into circularity when we consider that, through the taxation system, those that provide financial assistance for that private service (the public entity) may well receive the bulk of their money from those (the citizens) who also receive the same private services (the customers). Still, these reasonings might well be worth exploring and taking note of, when it comes to public policing on security spending allocation.

Private firms are extremely reluctant to comply with disclosure provisions about their cyber risks and incidents: They often prefer to pay the fines in exchange for their silence. This is why economic sanctions should be far graver, and complemented by administrative hurdles for those that do not obey the rules: for recurrent misbehaviour, it could be said that beyond charging the incompliant business with higher taxes (including insurance-related), that business could be liquidated altogether or gradually forced into compliance by name-and-shame actions, hostile secondary legislation as well as deterioration of its user-base. Rightly so: only the State can see the broader picture; e.g. in terms of reputation, a single company is concerned with the brand appeal disaffection which comes out of a major communication crisis,[208] whereas the public authorities may look at the systemic advantages of disclosure. If attracting investments is, before anything else, a matter of reputation and credibility,[209] when a country is unable to protect the assets of its own industries, no foreign (mainly direct) investment will reach that country: there is much to lose as indirect reputational damage, on the scale of the whole domestic systemic order, with concrete repercussions on the population's prospects. Obviously, all these considerations must be taken in aggregated shape, and are only valid as far as an idealized conception of an orderly "public" is put in place; unfortunately, widely known phenomena of corruption, inefficiency and regime selfishness relativize these claims with substantial practical reservations. At any rate, "IP theft differs from customer information theft in that [the] company owns the

scholarship on "stakeholder capitalism" (or "stakeholder theory of capitalism"). *See, e.g.*, Franklin Allen, Elena Carletti, and Robert Marquez, *Stakeholder Capitalism, Corporate Governance and Firm Value* (EUI Working Papers, No. 2009/10, 2009); R. Edward Freeman et al., Stakeholder Theory: The State of the Art (2010); Shinichi Hirota, Corporate Finance and Governance in Stakeholder Society: Beyond Shareholder Capitalism (2015); Robert Phillips, Stakeholder Theory and Organizational Ethics (2003).

208. There is often a public relations concern if news of trade secret misappropriation becomes public, particularly for publicly-traded companies whose stock (share) prices may be negatively affected.

209. Conceivably, the best evidence to support this statement comes from the international investment law regime. *See* Christopher M. Ryan, *Discerning the Compliance Calculus: Why States Comply with International Investment Law*, 38(1) Ga. J. of Int'l and Comp. Law 63, 94 (2009). *See also* U.N. Conf. on Trade and Dev., The Role of International Investment Agreements in Attracting Foreign Direct Investment to Developing Countries, U.N. Doc. UNCTAD/DIAE/IA/2009/5, at 25 (Sep. 2009).

IP . . . Because of this, [it] may very well have an obligation to *shareholders and stakeholders* to identify what has been stolen [and] assess potential impact."[210]

An alternative view with similar effects is to consider increasing taxation for noncompliant companies as a form of "social insurance" against the low-return value of the money-credit they borrow meaninglessly from the social body (the state administration); such a taxation also serves as an income redistribution (from companies to the community) and risk reallocation (from States back to their companies themselves) mechanism. Self-evidently, such a mechanism is conceived for democratic or however power-accountable regimes, where the "State" broadly coincides with the "community" rather than with an autocratic regime moved by its own interests detached from those of the society. Although in a perfect monopolistic system the aforementioned mechanism would unleash a dynamic of congestion pricing,[211] it shall be applicable to market economies; in this sense, it is increasingly adaptable to countries like China as they move towards embracing capitalism. Digging deeper into the issue, one may operate a distinction between profit and non-for-profit businesses, or between community-oriented and private services. For instance, if the noncompliant entity is a major industrial conglomerate (e.g. in transportation, health, schooling, etc.) offering irreplaceable public services, the economic damage arising from the avoidable stealing of trade secrets should be calculated on the basis of the loss as declared in the corporate-income-based entry of the general tax revenue per capita. Indeed, such a loss represents a burden for the taxpayers, to be translated in either increased public spending or increased taxation in order to guarantee the same level of service.

As far as general institutionalism is concerned, public trust is regarded as a positive *and necessary* attribute of any governmental exercise, making it possible for the executive to perform certain actions (e.g. law enforcement) while being generally supported and trusted by the population.[212] However, business-wise, trust can be reconceptualized *publicly* under a far less favorable light. As for "capitalising (on) trust", it might be worth decontextualizing a theory of intra-business efficient communication. Production and accumulation of trust can be regarded as a kind of human capital whose cost is shared by the networked parties involved, and that possesses certain attributes of a *public* good. Trust, to impact policymaking positively, should be horizontal (stakeholder-to-stakeholder) and never perfectly vertical: one might go as far as to claim that trust is nothing else than the culpably, disengaged *institutional*

210. Fancher, *supra* note 103 (emphasis added).

211. Definable as a pricing strategy elaborated to regulate demand by increasing prices whilst leaving supply unaltered.

212. Benjamin Goold, *Technologies of surveillance and the erosion of institutional trust*, in TECHNOLOGIES OF INSECURITY: THE SURVEILLANCE OF EVERYDAY LIFE 208 (Katja Franko Aas et al., eds., 2009).

production of an insecurity object. In other words, state administration should *check*, not trust: auditing and inspection are to be preferred, in that vertical suspicion provides wider room for horizontal trust and integrity.[213] For instance, the State may allow—or if allowed already, allow tax-free—investments (capital shares) in third companies only if the latter adopt cyber-hygiene precautions to protect trade. More lightly, it can be decided that the interest paid by noncompliant companies on their debts does not count towards tax deduction.

This should not lead to state over-bureaucratisation, and the balance to be kept between security and freedom is in fact a difficult one to pursue in practice. State suspicion must be channelled proactively and constructively for the greater good, rather than oppressively: Deterrence-based systems focus on *individual* motivation by prescribing sanctions, whereas compliance-based systems focus mainly on *organizational* routines for denying opportunities for deviant behavior as well as ensuring conformity to organizational goals. In contemporary times shaped by blurred boundaries between private risk management and public security,[214] deterrence- and compliance-based policies are as close to each other as never before: private organizations and their managerial practices—their internal risk management and control—are being conceptualized and operationalized as a security resource. The case of cyberattacks to nuclear plants—civilian and military alike[215]—exemplifies this convergence at its best. We agree in principle on the importance "to separate trade secrets which are company internal secrets, from classified information which is under governmental protection and regulation through national security acts,"[216] and yet, the two increasingly coincide or at least partly overlap.[217] One should bear in mind that, after all, stricter cybersecurity measures would burden companies on one side, yet freeing them on the other: cyber-hygiene and IT protection render employees' screenings less necessary or burdensome, preventing chilling effects on knowledge-circulation and experience-sharing from jeopardizing one's ability of benefitting from employers' skills and background in

213. For a partly dissenting view, *see* Randall Peerenboom, China modernizes: Threat for the West or Model for the Rest? 37 (2007).

214. *See generally* James P. Farwell, *Industry's Vital Role in National Cyber Security*, 6(4) Strategic Study Q. 10 (2012).

215. Rajesh M. Basrur, Minimum Deterrence and India's Nuclear Security, 132 (2009).

216. Lasse Øverlier, Intellectual Property and Machine Learning: An Exploratory Study 20 (Jan. 2017) (unpublished M.Sc. thesis at the Norwegian University of Science and Technology).

217. This is equally true on the criminals' side: public-owned Chinese companies in the defense and aerospace industries are actively involved in state-backed trade secret stealing campaigns. Nicholas Eftimiades, *Uncovering Chinese Espionage in the US*, The Diplomat (Nov. 28, 2018), https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us [https://perma.cc/MQ9G-SJWJ]. The danger comes from the fact that world market oligopolists like Airbus (Europe) and Boeing (U.S.) design and assemble aircrafts for the civil aviation and defense industry alike.

other companies; put simply, if IT protection is enhanced, the law can leave employees freer to capitalize on their talents and cumulated expertise in other companies (even direct competitors) once they have left a job position. As proving a breach of nonconfidentiality agreements is, for any former employer, an outcome-uncertain and time-consuming commitment,[218] preventively enhancing IT security is a win-win solution (and in public terms, more forward-looking a growth strategy). Enforcing noncompete agreements can be challenging as well, due to reasonableness and antitrust requirements.[219] Eventually, attaching too burdensome requirements on employees risks chilling their motivation to strive for knowledge they will be able to capitalize on: employees cannot unlearn what they know or they themselves produced as they can be prevented from downloading a file,[220] therefore the law should prioritize making the wilful stealing of proprietary information impossible.

Alongside due deference to (i.e. *binding* compliance with) current international standards on auditing in the public sector, the introduction of a new one on cybersecurity management and trade secret protection is hereby suggested—for example, the EU could readapt its eIDAS Conformity Assessment Report. Indeed, an audit is not simply a neutral check of conformity to independently derived performance standards; rather, it holds the power to shape those standards according to its own logic, which is exactly what lies behind his attraction as a macropolicy instrument. Similar to the practice of environmental compliance,[221] what matters is not the absolute value but the performance-based *process* of constant improvement.

It goes without saying that public finance should be employed to promote the public interest, that is, to serve the community as a whole: value-for-money requires both cost-effectiveness and outcome-effectiveness to be accomplished. Companies should be asked this all in a gradual and size- or capacity-tailored manner, without imposing undue burden which risks running contrary to the stated expected outcome, i.e., which limits business rather than making it flourish.[222] Whilst legislators and elected executives may settle the broader questions of distribution and of costs and benefits—and this settlement varies widely from jurisdiction

218. Daniel C. K. Chow, A Primer on Foreign Investment Enterprises and Protection of Intellectual Property in China 189 (2002).

219. Pamela Carder Fletcher, *Antitrust Implications Arising from the Use of Overly Broad Restrictive Covenants for the Protection of Trade Secrets*, 29(2) Hastings L.J. 297, 303–308 (1977).

220. William van Caenegem, Trade Secrets and Intellectual Property: Breach of Confidence, Misappropriation and Unfair Competition 35–36 (2014).

221. Marie-Gabrielle Piketty and Isabel Garcia Drigo, *Shaping the implementation of the FSC standard: the case of auditors in Brazil*, 90 Forest Pol'y and Econ. 160, 164 (2018).

222. Rowe, *supra* note 41, at 410.

to jurisdiction—it is left to public administrations to wrestle with the smaller question of fairness and equity in every individual case.[223]

VI. Views from the United States of America

> *Inventing new and better technologies, production methods, and the like, can be expensive. American companies and the U.S. Government spend billions on research and development. The benefits reaped from these expenditures can easily come to nothing, however, if a competitor can simply steal the trade secret without expending the development costs. While prices may be reduced, ultimately the incentives for new invention[s] disappear, along with jobs, capital investment, and everything else that keeps our economy strong*.[224]

Over more than two decades, in spite of the novel legislative efforts outlined both *supra* and *infra*, little has changed in practice for U.S. trade secret owners and America's "innovation backbone." This notwithstanding, differently from areas such as privacy, environmental protection or competition in digital services, where the EU is arguably championing the West-led normative discourse globally, the United States is to be taken as benchmark as far as trade secret protection from a "Western" standpoint. Indeed, if one compares the U.S. framework with the European one,[225] a landmark achievement of the former is the criminalization of the thief;[226] this is essential, considering how a low-level employee might otherwise benefit from a benefit-risk ratio which situates the worse-case scenario in a civil compensation (which most of those low-level employees would be unable to pay anyway).[227] We deem criminalizing thieves a step in the right direction as far as it operates on deterrence;[228] however, enforcement hurdles related to this form of deterrence when it comes to *international* thefts, make a deterrent approach *based instead on obligatory minimum levels of cybersecurity* highly warranted (save that the two deterrence rails—criminalization and cybersecurity—are not mutually exclusive). Economically, criminalization "might make matters worse by

223. *See generally* Blue Wooldridge and Betsy Bilharz, *Social Equity: The Fourth Pillar of Public Administration*, *in* Global Encyclopedia of Public Administration, Public Policy, and Governance (Ali Farazmand ed., 2017).

224. 142 Cong. Rec. S12207-08 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

225. *See generally* Yana Daluchi Somkenechi Madubuko, The protection of Trade Secrets: A Comparative analysis of the United States and the European Union (2018) (unpublished B.A. thesis, Tallinn University of Technology).

226. For the details on these criminal provisions at the federal and state levels, *see* Kurt M. Saunders, and Michelle Evans, *A Review of State Criminal Trade Secret Theft Statutes*, 21(2) UCLA J. of L. and Tech. 1 (2017).

227. Shreya Desal, *SHHH! It's a Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive*, 46(2) Ga. J. of Int'l and Comp. L. 481, 512 (2018).

228. On the justifiability and advisability of deterrence-based rationales for criminalizing IP thefts, *see* Andrea Wechsler, *Criminal enforcement of intellectual property law: An economic approach*, *in* Criminal Enforcement of Intellectual Property 135–138 (Christophe Geiger ed., 2012).

adding more in enforcement costs than it saves on indirect and transaction costs":[229] for all these reasons altogether, intervening on the owners rather than on the potential and alleged stealers seems more fruitful and cost-efficient a path for the State.

Sharing information on possible cybersecurity risks among companies could increase their security and prevent a share of thefts, but it is not immune from risks, including legal ones.[230] Promulgated in 2015, the Cybersecurity Act includes a Cybersecurity Information Sharing Act (CISA) "designed to foster cyberthreat information sharing and to provide certain liability shields related to such sharing and other cyber-preparedness."[231] With this Act, the Government recognizes its central role, and de facto asserts that company liability for cybersecurity unpreparedness cannot be attributed if the Executive itself was inattentive in designing up-to-standard policies and facilitating the sharing of good practices, "with attention to accessibility and implementation challenges faced by small business concerns."[232] Data protection and incident management laws are applied (at times sector-specifically) on a State-by-State basis, with no overarching federal statute other than those specifically covering three sectors: healthcare, finance, and telecommunication. As per the interaction between trade secrets as an IP system and trade secrets as security device, Obama's "Executive Order 13694 marked a significant policy change by authorizing sanctions against individuals or entities involved in certain significant cyberattacks originating from or directed by individuals abroad considered a significant threat to the national security, foreign policy, or economic health or financial stability of the United States": this potentially covers trade secrets thefts, although the categories of intended crimes to be addressed is left vague.[233] From 2009–2012, the U.S. Department of Justice charged nearly 100 entities with stealing trade secrets and unlawfully exporting technology controlled by the US International Traffic in Arms Regulation or the Export Administration Regulations;[234] the export frequently follows the

229. Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86(2) Calif. L. Rev. 241, 276 (1998).

230. Baker, *supra* note 86, at 257–259.

231. Raul, *supra* note 142, at 383.

232. Cybersecurity Information Sharing Act, S. 754, 114th Cong. § 103(a)(5) (2015).

233. Anthony V. Capobianco, et al., International Trade Regulation and Cybersecurity, Lexology (Apr. 22, 2016), https://www.lexology.com/library/detail.aspx?g=892b4b55-bab3–490e-8bd7–837ac7d81ea0 [https://perma.cc/HW7E-9UY5]; see also Deen H. Kaplan, et al., International Trade Regulation and Cybersecurity, Hogan Lovells (Apr. 26, 2016), http://ehoganlovells.com/rv/ff0026f4dbb4ce131fb8547fb144862f7c27241b.

234. Covington & Burling LLP, *Chinese National Sentenced to Nearly Six Years in Prison for Illegally exporting U.S. Military technology*, Covington (Mar. 31, 2013), https://www.cov.com/-/media/files/corporate/publications/2013/03/chinese_national_sentenced_to_six_years_for_illegally_exporting_us_military_technology.pdf [https://perma.cc/QZG6-K9KD].

theft, as the stolen trade secret is used to rapidly engineer dual-end technology destined to benefit authoritarian foreign powers.

Other U.S. legislative and executive solutions to trade secret misappropriation have found shore in, among others: Computer Fraud and Abuse Act (1984),[235] Uniform Trade Secrets Act (1985), Economic Espionage Act (1996), Theft of Trade Secrets Clarification Act (2012), Penalty Enhancement Act (2013), Report "Summary of the Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases" (2012), "Obama Administration Report on Trade Secrets" (2013), and the proposed Protecting American Trade Secrets and Innovation Act (2012) and Cyber Intelligence Sharing and Protection Act (2015). In 2016, the US government enacted the Defend Trade Secrets Act.[236] An extremely extensive and all-encompassing amount of academic and nonacademic literature covered these provisions in distinguished detail already;[237] as such, the present analysis will gloss over them to immediately pivot to the Indo-Pacific macroregion. The analytical endeavour will scrutinize *preventive* cybersecurity laws which might potentially have an impact on *preventive* trade secret protection.[238] It will be demonstrated that, paradoxically, the US legislation is closer to the Chinese one than to the Japanese, Indian, or Australian ones, although these three legal orders often claim or implicitly assume to adopt a roughly Western orientation.

VII. The Indo-Pacific region: Insights From China, India, Japan, and Australia

A. *Mainland China*

Art.24 of the amended (2012) PRC's Labour Contract Law and Art.62 of the amended (2004) PRC's Company Law bind companies' senior management to be loyal to their companies in refraining from disclosing sensitive information.[239] Art.80 of the latter piece of legislation prescribes that the amount of capital contributions made by sponsors in

235. On the application of this provision to trade secret cases, *see* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two problems and two solutions*, 2 U. Ill. J.L. Tech. & Pol'y 429 (2009).

236. For an analysis, *see* Daixi Xu, and Brent Caslin, Trade Secrets Venue Considerations, American Bar Association (Feb. 7, 2017), https://www.americanbar.org/groups/litigation/committees/intellectual-property/articles/2017/trade-secrets-venue-considerations [https://perma.cc/43VY-V7Y2].

237. Among many others, *see, e.g.*, Villasenor, *supra* note 56, at 337–40; van Caenegem, *supra* note 220; Keren Livneh and Jacob Reed, *USA*, *in* The International Comparative Legal Guides (Nigel Parker et al., eds., 2019); David R. Fertig, Christopher J. Cox, and John A. Stratford, (2015) *The Defend Trade Secrets Act of 2015: Attempting To Make a Federal Case Out of Trade Secret Theft—Part I*, 1(2) Pratt's Privacy and Cybersecurity Law Report 60 (2015); Robert C. Denicola, *The New Law of Ideas*, 28(1) Harv. J.L. & Tech.195 (2014).

238. For an overview of these measures, *see* Livneh, *supra* note 237 at §§ 2.3–2.11.

239. Xiong, *supra* note 3, at 268 n. 64; 269 n.66.

the form of industrial property rights and nonpatented technology shall not exceed twenty percent of the registered capital of a joint stock limited company.[240] This was a wise move to reduce risks and prevent failures wherever cyber hygiene is not—also due to financial constraints—duly implemented; it is advocated that this policy does not change for the time being, with the only exception of a special registry of innovative startups entirely based on innovative (by product, process, or a combination thereof) business models. This is even more important since 27 October 2005, when the Chinese Standing Committee of the National People's Congress adopted major revisions to China's company law, including the introduction of one-person companies and lower capital requirements: for limited liability companies, the minimum capital has been decreased from RMB 100.000 to RMB 30.000. A one-person company could be set up with a minimum capital of 12.500 U.S. dollars. "[A]s politicians and business groups across Asia reflect on the changes in Japanese company law, which are seen as offering organizational advantages to firms in knowledge-intense industries, lawmakers in other Asian competitive countries such as India, Malaysia and China are already sequencing reforms that will lead to the introduction of the [limited-liability-partnership structure]."[241] One may conclude that although China is generally known for large corporations well tied with the State, corporate registration has been slimmed, and nonpatented IP has been placed at the center of protection policies. Also, state ownership is a truth but should not be overemphasized: already two decades ago it was made no secret that "the owners of private companies in China ha[d] already developed into a social stratum with relatively independent social-economic status and political demands . . . acknowledged [. . . and] recognized [by the Party]."[242]

In compliance with China's Anti-unfair Competition Law (1993, amended 2017), Several Provisions on Prohibiting Infringements upon Trade Secrets (1998) and the Judicial Interpretation of the Supreme People's Court on Matters About the Application of Law in the Trial of Civil Cases Involving Unfair Competition (2007), show that "reasonable confidentiality measures shall not only reflect the rightsholder's intention about what information they wish to keep confidential, but also have concrete manifestation; and the specific confidentiality measures shall also have the effect of preventing classified information from being disclosed under normal condition."[243] On the other side, the just-revised

240. Vai Io Lo & Xiaowen Tian, Law and Investment in China: The Legal and Business Environment After China's WTO Accession 36 (2004).

241. Joseph A. McCahery & Erik P.M. Vermeulen, Corporate Governance of Non-Listed Companies 103 (2008).

242. Xiaojun Feng, *Dramatic demonstrations to demand back wages: The logic of practice of informal defenses of legitimate rights*, 12 Rural China: An Int'l J. Hist. & Soc. Sci. 156, 163–164 (2015).

243. *Strategies for Trade Secrets Protection in China*, AFD China (2018), http://afdip.com/index.php?ac=article&at=read&did=3212 [https://perma.cc/W7R4-HQ3T].

(April 2019) Art.9 of the mentioned Anti-Unfair Competition Law (which, although centered on consumer protection, is the primary reference for trade secrets provisions in China[244]), spells out a novel type of trade secrets infringement, namely the cyber-enabled one.[245] This update, together with the new Cybersecurity Law, indirectly turned an overall fragmented[246] and weak trade secrets protection system[247] into the most secure (on paper, at least) in the world: irrespective of the truth that IPRs "in China are unevenly and somewhat arbitrarily enforced,"[248] trade secrets (or at least the digital ones) are now protected, paradoxically, by means of a law which has *prima facie* nothing to do with the protection of intellectual property.

One should stand up vigorously against all those who claim that Chinese cybersecurity laws are a fiction: not only are they extremely advanced and not vaguer if compared to those in the Pacific region, but also, implementation gaps are less evident here than in other policy areas in China. Although the aim of these laws was more about surveillance than protection of trade secrets, they incidentally ended up serving the second function as well (as far as *international* thefts are concerned); this work will not dig deeper into the first function, as it is already explored in literature.[249]

Even before the current cybersecurity regime came into play, the 2010 Administrative Measures for the Security Protection of Communication Networks specified that "the staff of the Telecommunication

244. Eric D. Engelman, *Burdensome Secrets: A Comparative Approach to Improving China's Trade Secret Protections*, 25 Fordham Intell. Prop., Media & Ent. L.J. 589, 598 (2015). *See also* Guangjie Li, Revisiting China's Competition Law and Its Interaction with Intellectual Property Rights 26 (2018).

245. *See generally* Laney Zhang, *China: Trade Secret Provisions Under Anti-unfair Competition Law Revised*, Global Legal Monitor (2019), https://www.loc.gov/law/foreign-news/article/china-trade-secret-provisions-under-anti-unfair-competition-law-revised.

246. *See generally* Xiong, *supra* note 3, at 254–55; 269–73.

247. *See* Daniel F. Roules, *What is the Greatest Risk to Your Trade Secrets in China?*, A round-up of Labour and Employment stories from around our global network (2013), https://www.lexology.com/library/detail.aspx?g=819663e7-944c-45a1-94ce-5a834b1f7330 [https://perma.cc/Q7X4-2MB9] (follow the "View original" hyperlink).

248. Dan Breznitz & Michael Murphree, *China's Run—Economic Growth, Policy, Interdependences, and Implications for Diverse Innovation Policies in a World of Fragmented Production*, *in* The Third Globalization: Can Wealthy Nations Stay Rich in the Twenty-First Century? 35, 44 (Dan Breznitz & John Zysman eds., 2013).

249. *See, e.g.*, Steve Dickinson, *China's New Cybersecurity System: There is NO Place to Hide*, China Law Blog (Oct. 7, 2019), https://www.chinalawblog.com/2019/10/chinas-new-cybersecurity-system-there-is-no-place-to-hide.html [https://perma.cc/3D52-MH4X]; Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State*, 30 J. Democracy 53, 53–67 (2019); Zhuang Pinghui, *China pushes through cybersecurity law despite foreign business fears*, South China Morning Post (Nov. 7, 2016, 3:45 PM), https://www.scmp.com/news/china/policies-politics/article/2043646/china-pushes-through-cybersecurity-legislation-heavily [https://perma.cc/MMD8-CURX].

Administrative Authority, which [wa]s made up of the Ministry of Industry and Information Technology and Communication Administrative Bureaus, [had] the obligation to maintain the confidentiality of state secrets, *trade secrets* and personal secrets that c[a]me to their knowledge in the course of inspection."[250] According to the new Cybersecurity Law of 1 June 2017, the failure to prevent, mitigate, manage or respond to incidents results in the person(s) in charge being fined. Any unattendance of the Party's concerns under Art.286(1) of the PRC's Criminal Law translates into the network operator fined and its administrators sentenced; this is of the utmost importance, as the previous criminal provisions applicable to trade secret thefts left it unclear "whether the loss of a trade secret [was] calculated on the basis of the loss to the owner of the trade secret or the loss of the value of the trade secret itself. In addition, it appears [there was] no distinction between intentional, accidental, or inadvertent infringement."[251] The mentioned Cybersecurity Law further calls for *compulsory* designation of CISO, emergency plans, monitoring, and recordkeeping; its Art.38 compels the execution of a yearly major security assessment, whose results shall be forwarded to the competent central authorities (this is a self-assessment; yet, third parties may get involved under certain conditions). In keeping with the Information Security Techniques—Personal Information Security Specification (recommended—although "understood as binding"—standards[252] formulated by the National Standardisation Committee), operators shall at least inform data subjects of the general description of the incident along with its impact, any remedial measure taken or soon to be adopted, suggestions for those whose data has been violated, contact information, and details on cooperation with public authorities.

To the surprise of many, China seems at the same time one of the greatest stealers of trade secrets in human history, and a jurisdiction where the protection of their own ones is taken seriously, especially in the cyber dimension. As China is right on the edge between developing status (in its inner lands) and superpower projection (along the coastal line, including the Greater Bay Area with the two S.A.R.s Hong Kong and Macao), no expert can be caught off-guard: "many so-called 'developed countries' have undergone periods of rampant violations of the IP rights of other countries, including European states, *the United States*, Japan and Taiwan, before they turned into countries pushing for increased IP protection and enforcement."[253]

250. James D. Fry, *Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. Pa. J. Int'l L. 419, 494 (2015) (emphasis added).

251. Xiong, *supra* note 3, at 274–75.

252. *See* Samm Sacks & Manyi Kathy Li, *How Chinese Cybersecurity Standards Impact Doing Business in China* 11, Center for Strategic and International Studies (Aug. 2, 2018) https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china [https://perma.cc/W4VT-22BR].

253. Rostam J. Neuwirth, *Counterfeiting and Piracy in International Trade: the Good, the Bad and the . . . Oxymoron of "Real Fakes,"* 7 Queen Mary J. Intell. Prop.

B. *India*

Noncompliance with India's Information Technology Act (2000) cybersecurity requirements may amount to a breach of directors' duties under the Companies Act (2013). The former's Sec.85 mandates the liability of company high managers for not designating a CISO, establishing cyberattacks response procedures, conducting extensive risk assessments, and performing penetration and/or vulnerability assessments. *Companies with over a thousand shareholders* must ensure the security of electronic records (Companies Rules 2014, Nos. 20;28), including: protection against unauthorized access, alteration or tampering; security of computer systems, software and hardware; periodic backup; empowerment of computer systems as to discern invalid/altered records; and retrievable of readable/printable records. Yet, usually fines are imposed for breaching privacy laws instead. Moreover, no penalty is prescribed for noncompliance with the mandatory reporting of incidents (ITA, Sec.34), although this might change soon as Art.32 of the *Draft* Personal Data Protection Bill 2018 foresees the possibility of penalties and requires the performance of both incident impact assessments and recordkeeping.

Nevertheless, in a country where corruption is endemic, and the judicial review of governmental choices in competition law and other fields remains at best elusive if not nonexistent altogether, prevention is particularly necessary: when a trade secret theft occurs, Indian companies prefer to stage criminal cases (based on Secs. 405;408;418;420 of India's Penal Code) over civil ones exactly because the latter are corrupted and lengthier, even if a civil case is the only way to obtain a court injunction; this way, a criminal trial only serves as an intimidation mechanism for further thefts on an individual level, without the ability to economically redress the stealing of the trade secret.[254]

C. *Japan*

In June 2004, the Act for Establishment of the Intellectual Property High Court was enacted, whereupon the Intellectual Property High Court was set up, commencing its works in April 2005.[255] However, cases of infringement of intellectual properties of Japanese corporations, especially from China, are increasing at speed rate.[256] This is such a largescale phenomenon that it concerns not only the victimized corporation but also the theft of the overall technological "assets package" of Japan, making its society poorer and less motivated to continuously innovate. The damage caused by Chinese corporations, in 2001 *only*, has been set to 2.7

L. 444, 453 (2017) (emphasis added).

254. *See* Prashant Reddy T., *The 'Other IP Right:' Is It Time to Codify the Indian Law on Protection of Confidential Information?*, 5 J Nat'l L.U. Delhi 1, 14 (2018).

255. *See generally* Katsumi Shinohara, *Outline of the Intellectual Property High Court of Japan*, AIPPI J. 131, 131–47 (2005).

256. *See* U.S. Int'l Trade Comm'n, China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy no. 4226, Investigation No. 332–519, at 2–5 (2011).

trillion yen, and even the Chinese government itself admitted that "the total market value of counterfeits [that year] was somewhere between 2.2 and 2.8 trillion yen."[257] Infringements of intellectual properties of Japanese corporations centering on damages caused by imitation products—like "Japanese-sound products"—are so overwhelming that taking legal action (and waiting long times for the courts' decisions) no longer makes sense. "Transnational [c]orporations and [S]tates are constantly operating within a volatile industrial and technological environment in a space and time-shrinking era,"[258] and mentioned unreliability of—and nonreliance on—judicial (and even extrajudicial) settlements is one of the prominent features of today's overcongested acceleration. Against this backdrop, protecting hidden assets like trade secrets seems to be the only possible solution, as they prove increasingly strategic to retain a residual "competitive advantage" based on economic creativity. It is now possible to see why the approach adopted by Japanese courts—that of requiring "companies to take seemingly extraordinary measures to protect their trade secrets"[259] by "limit[ing] the number of people with access to the information, giv[ing] clear notice that the subject matter is secret, and implement[ing] physical and electronic access restrictions"[260]—is a farsighted one. Trade secrets are so irreplaceable for Japanese companies that the latter do not even venture in cooperating with Japanese universities, due to fears of inappropriate disclosure of these IP assets.[261]

Japan's Companies Act speaks of "due care as a prudent manager" in the good conduct of businesses; overall, Japanese legal language about cybersecurity and data protection is in fact soft and liberal. The IT Promotion Agency, jointly with the Ministry of Economy, Trade, and Industry, has issued Cybersecurity Management *Guidelines* aimed at *recommending* risk management procedures to be put in place. The Financial Services Agency's Guidelines includes among the relevant standards for banks: the constitution of an emergency unit; the appointment of a specific manager; and the recourse to periodic assessments. Nevertheless, these indications are not

257. Hisamitsu Arai, *Intellectual Property Strategy in Japan*, 1 Int'l J. Intell. Prop. 5, 9 (2005).

258. Kogila Balakrishnan, *The Rationale for Offsets in Defense Acquisition from a Theoretical Perspective*, *in* Emerging Strategies in Defense Acquisitions and Military Procurement 273 (Kevin Burgess & Peter Antill eds., 2017).

259. Orrick, Herrington & Sutcliffe LLP, *"We're Not Gonna Take It!" Significant Changes to Japan's Trade Secret Protection Law*, Trade Secrets Watch (Apr. 18, 2016), https://blogs.orrick.com/trade-secrets-watch/2016/04/18/were-not-gonna-take-it-significant-changes-to-japans-trade-secret-protection-law [https://perma.cc/8M5U-VQCJ].

260. Pamela Passman, *Trade Secrets: The "Reasonable Steps" Requirement*, Intell. Prop. Watch (Aug. 19, 2015), https://www.ip-watch.org/2015/08/19/trade-secrets-the-reasonable-steps-requirement [https://perma.cc/C9KT-XUVS].

261. *See* Smriti Mallapaty, *Japan's Start-Up Gulf: Academia and Industry in Japan Remain Disconnected, Despite Efforts to Bring Them Together*, Nature (Mar. 20, 2019), https://www.nature.com/articles/d41586–019–00833–3 [https://perma.cc/X7LZ-CY9B].

binding and fail to mention incident disclosure requirements[262] or specific cybersecurity measures to be preventively implemented. This voluntary approach follows throughout all other relevant pieces of public legislation and private regulation. The Act on the Prohibition of Unauthorized Computer Access (1999, lastly amended in 2013) talks of making "any effort to protect . . . ". The Basic Act on Cybersecurity's suggestion is to *voluntarily* and proactively enhance cybersecurity, and to collaborate with governmental apparatuses. In November 2018, an Amendment to the Telecommunication Business Act was approved, in order to enable (. . . yet, not to compel) telecom carriers to share cyberattack information with industry competitors.

D. *Australia*

In Australia, there can be Commonwealth-wide, state, and territory crimes. Unlike States and territories, which have general legislative power for the "peace, order and good government" of their respective jurisdictions, the Commonwealth of Australia's legislative power is limited to prescribed topics, such as international and interstate trade and commerce, taxation, corporations, external affairs, currency and banking, intellectual property, etc.[263] There is no general legislative power with respect to criminal laws, which are traditionally a state and territory matter; however, the Commonwealth can enact criminal offenses in relations to its particular legislative competencies.[264] Thus, commonwealth offenses exist in relation to corporate misconduct, some forms of fraud, telecommunications, crimes against internationally protected persons, terrorism, copyright piracy and trademark infringement. All those may be executed through computers and similar devices.[265]

Australia's Corporations Act (2001) is rightly considered outdated. On the failure to prevent, mitigate, manage, and respond to cyberthreats, it imposes duties on directors to exercise powers with the care and diligence a reasonable person would. A director who ignores the real possibility of an incident may be liable for failing to exercise reasonable due diligence.

262. With an exception, though: the Guidelines released by the Personal Information Protection Committee require telecom operators (exclusively!) to promptly submit a summary of the occurred breach plus a list of the measures taken thereafter; this is limited in two ways: recommendations are obviously nonbinding in nature, and in this case, they fail to *prevent*, rather implementing the lexicon of *recovery*.

263. *See generally* Nicholas Aroney, The Constitution of a Federal Commonwealth: The Making and Meaning of the Australian Constitution 276 (2009); Joe Edwards, *Applied Law Schemes and Responsible Government: Some Issues*, *in* Law and Democracy: Contemporary Questions 85–112 (Glenn Patmore & Kim Rubenstein, eds., 2014); Nicholas Aroney, Peter A. Gerangelos, Sarah Murray & James Stephen Stellios, The Constitution of the Commonwealth of Australia: History, Principle and Interpretation (2015).

264. *See generally* Francine Feld, Andrew Hemming & Thalia Anthony, Criminal Procedure in Australia (2014); Mark Findlay, Stephen Odgers & Stanley Yeo, Australian Criminal Justice (5th ed. 2014).

265. *See generally* Austl. Inst. of Criminology, Pub. No. 94, Intellectual Property Crime and Enforcement in Australia (2008).

This all sounds good; however, at a closer inspection, it unveils its vagueness and shortcomings. The Act does not oblige companies to designate a CISO, to draft a written incident response plan/policy/guideline, to conduct periodic cyber risk assessments, or to perform penetration tests or vulnerability assessments (by way of comparison, in India these steps are mandatory for banks, financial operators, insurance companies, as well as telecom companies). The more recent Privacy Amendment Act (February 2018) established that notice of an "eligible data breach" (under the Notifiable Data Breaches Scheme) to central regulatory authority *and* affected individuals shall be provided. This is a move in the right direction, but fails insofar as it is not applicable to small businesses, which should be protected *a fortiori*. If compared to big corporations, small businesses—and especially startups—are more innovation-dependent, less financially endowed to manage patents,[266] more exposed to cyber threats, and more subject to "internal misappropriation" due to less formal employment contracts and less stringent hierarchical oversight. Two other considerations are warranted here: first, startups are more strategic to invest in innovation-wise, as their business plan relies on economy of scale (rapid scalability) models; second, cyber insurances are typically more burdensome on investment-driven and young companies, which in turn, need to stipulate wider-encompassing insurance contracts.[267] In sum, prevention is favorable for big corporations, but *essential* when it comes to innovative SMEs. Australia has no uniform statute on breach of confidentiality (as a tort) in place; however, some parts of the 1995 Criminal Code Act (Commonwealth's penal code) do address the issue on the criminal side: Sec.478.1 on cyber-intrusion and electronic theft; Sec.477.3 on DDoS; Sec.478.2 on malware infection; and Sec.478.3 on the possession of hacking tools. These provisions "reflect the principle of 'online-offline consistency' where the regulation of unlawful conduct in cyberspace is made consistent with the regulation of unlawful conduct in the physical realm."[268]

Generally, however, Australia got it wrong (if not illegal) to its worst: "[a] trade secret is proprietary knowledge and it is up to you to protect that knowledge," its Government boldly proclaims in writing.[269] To the

266. As per exemplifying, an official survey has revealed that almost the 77 percent of Finnish SMEs relied on trade secrets to protect their IP assets. Siivonen, *supra* note 48, at 7.

267. One must note, however, that both conceptually and practically, insurance is a cure, not a solution. It materializes once the harm has occurred, whereas—as clarified several times throughout this Article—the true added value of a trade secret stands with its irreplaceability as a nondisclosed asset. Differently from many other assets, its theft cannot be monetary compensated to a full extent. An insurance cannot restate the competitive environment as it existed before the infringement: Typically, it confines itself to provide (a lower amount than) the gains that according to some econometric projection the company would have acquired over a limited period of time, should the trade secret had remained in the ownership of the breached company.

268. Stephen Tully, *Protecting Australian Cyberspace: Are our International Lawyers Ready?*, 19 Australian Int'l L.J. 49, 68 (2012).

269. *Types of IP*, Austl. Gov't: IP Austl., https://www.ipaustralia.gov.

contrary, and despite upholding transparency as one of its key-values[270] (which, IP-wise, only patents can guarantee),[271] the TRIPS itself clarifies that "*Members* shall protect undisclosed information,"[272] and that assisting companies to protect their systems is the only way for the State to discharge its (international) duties.[273] This is confined to cases[274] where States require "as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort."[275] However, the concept underpinning this provision stands perfectly in line with the one this Article argues for more widely. What Canberra seems to forget is that trade secrets, from a macroeconomic perspective, are state assets just as much: conclusively, a more proactive role for the State should be advocated for, exactly to make businesses—in turn—more responsible about their IT-system protection and ultimately security-wise independent.

Further pieces of relevant legislation are, for example, the 1979 Telecommunications Interception Act, the 1995 Criminal Code Act, the 2001 Cybercrime Act, the 2004 Crimes Legislation Amendments, and the same year's Surveillance Devices Act. Like above, these will not be examined here, as the analysis will depart from purely domestic contexts to hint at private international law implications and eventually moor at the harbour of public international law.

VIII. The Transnational Dimension: Supply-Chain Networked Liability

The importance of trade secrets protection along supply chains has already been hinted at above: fragmented and uneven standards of protection across jurisdictions constitute a de facto barrier to trade,[276] so that

au/understanding-ip/getting-started-ip/types-of-ip [https://perma.cc/4S8C-DN45].

270. *See* TRIPS Agreement, *supra* note 7, at Art. 63.1. *But see* TRIPS Agreement Art. 63.4.

271. *See* John Braithwaite & Peter Drahos, Global Business Regulation 78 (2000).

272. TRIPS Agreement, *supra* note 7, Art. 39.1 (emphasis added). *See* Bently, *supra* note 11 at 1138. *See generally* François Dessemontet, *Protection of Trade Secrets and Confidential Information*, *in* Intellectual Property and International Trade: The TRIPS Agreement (Carlos M. Correa & Abdulqawi A. Yusuf, eds., 2nd ed. 2008); Pedro Roffe, Christoph Spennemann & Johanna von Braun, *Intellectual Property Rights in Free Trade Agreements: Moving Beyond TRIPS Minimum Standards* 226–316, *in* Research Handbook on the Protection of Intellectual Property under WTO Rules: Intellectual Property in the WTO (Carlos M. Correa ed., 2010).

273. *See* TRIPS Agreement, *supra* note 7, Art. 39.3 ("Members shall protect such data against disclosure . . . unless steps are taken to ensure that the data [is] protected against unfair commercial use.").

274. *See, e.g.*, Schultz et al., *supra* note 149, at 95 ("[m]any observers considered the TRIPS minimum standards too low").

275. TRIPS Agreement, *supra* note 7, Art. 39.3.

276. *See also* Alberto Oddenino, *Digital Standardization, Cybersecurity Issues and International Trade Law*, 51 Zoom-In, Questioni di Diritto Internazionale n.70

protecting trade secrets by means of *internationally standardized* cybersecurity measures helps keep trade fair and manageable,[277] averting, for example, non-tariff barriers as much as phenomena of supply-chain technological "decoupling."[278] Not by chance, scholars urge negotiators of trade and investment agreements to take the Trans-Pacific Partnership as a model,[279] in that it requires participating countries to both ensure they have adequate systems of prevention in place, and criminalize the theft of trade secrets.[280] Regrettably, the Regional Comprehensive Economic Partnership under negotiation between the ASEAN countries and its six FTA partners (China, Japan, India, South Korea, Australia and New Zealand)—or "ASEAN+6"—does not for the time being include in its draft any criminalization of trade secret thefts.[281] One might speculate that the geopolitically uneven membership of this agreement makes it difficult to compromise on the stances brought forward by countries as different as

(May 31, 2018) ("[The proposal] to deal with cybersecurity in the context of the World Trade Organization (WTO), finding viable solutions through an evolutionary interpretation, in particular, of the Agreement on Technical Barriers to Trade (TBT) . . . for a continuous development of common digital standards guaranteeing interoperability and openness of networks, and a fair balance of the interests involved, that also comprise the protection of trade secrets and IPR.").

277. For instance, in Europe, "[t]he fact that cases of infringement of trade secrets—whether by way of espionage or employees moving to other companies—frequently have cross-border references is one of the primary arguments in favor of legal harmonization. However, at present the legal systems of the [EU's] Member States differ significantly with respect to the systematics and the level of protection afforded to trade secrets. On the one hand, this renders legal enforcement more difficult in cases of infringement. On the other hand, *there is a risk of barriers to trade* within the internal market since the passing on of confidential information to other countries is impaired if it is not ensured that adequate legal protection is guaranteed in the target country and if there is a lack of clarity about the available means of redress." *See, e.g.*, The German Association for the Protection of Intellectual Property (GRUR), Opinion on *the proposal for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final*, 2 (Mar. 19, 2014), http://www.grur.org/uploads/tx_gstatement/2014-03-19_GRUR_Stellungnahme_zum_Know-how-Schutz_EN.pdf (emphasis added).

278. *See*, *e.g.*, Tung Chee-hwa, *The US and China complement each other: Decoupling doesn't make sense for either nation, or the world at large*, South China Morning Post (July 12, 2019), https://www.scmp.com/comment/opinion/article/3018013/us-and-china-complement-each-other-decoupling-doesnt-make-sense [https://perma.cc/C22M-J3GR] (on technological decoupling during the ongoing "trade war").

279. Peter f. Cowhey & Jonathan David Aronson, Digital DNA: Disruption and the Challenges for Global Governance 244 (2017).

280. However, after the US' withdrawal, this arrangement is far less influential. *See*, *e.g.*, Mona S. Amer, *Final TPP Language on Trade Secret Protection Disclosed*, Orrick: Orrick Blogs (October 22, 2015), https://blogs.orrick.com/trade-secrets-watch/2015/10/22/final-tpp-language-on-trade-secret-protection-disclosed [https://perma.cc/X9BM-GVPS]; Jon-Erik G. Storm, *Misconceptions about the TPP, Trade Secrets and Non-Compete Agreements*, Medium (August 6, 2016), https://medium.com/@stormj/misconceptions-about-the-tpp-trade-secrets-non-compete-agreements-32b8ee9d5f5e [https://perma.cc/Y735-QVZY].

281. *See* Peter K. Yu, *The RCEP and Trans-Pacific Intellectual Property Norms*, 50 Vand. J. Transnat'l L. 673, 715 (2017).

China and Australia (or New Zealand, where the expression "trade secrets" is not even granted a specific legal status[282]), including for the interventionist/liberal and hard/soft-law dichotomies outlined above with regards to the enforcement of corporate cybersecurity standards. Even those who do not attach any significance to the TPP "in providing a regional solution to the thorny piracy and counterfeiting problems," highlight its higher geopolitical coherence when compared to that among the RCEP members.[283]

Let us suppose there is a company A located in country AA and that because of company A's poor cyber hygiene or country AA's failure to legislate appropriately, an extremely strategic trade secret is stolen by company D situated in country DD from company A. A is part of a supply chain touching upon companies B and C in countries BB and CC. Clearly, poor cybersecurity measures in any link (A, B, or C) of the ABC chain cause business disruption (or even macro security vulnerability) all throughout the system.[284] As a matter of private international law, the damage suffered by companies in countries BB and CC depends on the form and validity of the contracts of all parties among themselves; in public international law terms, companies' liability under those contracts can internationalize, insofar as States decide the stolen asset to be so important to warrant an exacerbation of interstate relations through the diplomatic protection mechanism. Whereas two decades ago the international dimension of trade secret policing was already a reality,[285] it is now shifting from vertical forms of organization to horizontal interliability schemes. In 2014, Italy and France presented a proposal to UNCITRAL in order to introduce the "network contract"-model, that "not only offers the possibility of segregation of assets[286] and consequently limited liability protection, but also facilitates internationalization of MSMEs and cross-border cooperation. Moreover, it provides a tool to link MSMEs to larger companies by permitting MSMEs to be connected to the supply chain of such companies."[287] In other words, it allows for facilitated

282. *See generally* Rob Batty, *"Trade Secrets" Under New Zealand Law*, 22 Canterbury L. Rev. 235–268 (2016).

283. *See*, *e.g.*, Peter K. Yu, *A Spatial Critique of Intellectual Property Law and Policy*, 74(4) Wash. & Lee L. Rev. 2045, 2079–2089 (2017).

284. *See* Pamela Passman, *Inside Views: How To Safeguard Trade Secrets: Think ROI*, Intell. Prop. Watch (Mar. 17, 2014), https://www.ip-watch.org/2014/03/17/how-to-safeguard-trade-secrets-think-roi [https://perma.cc/V7UB-8CK6].

285. *See*, *e.g.*, Giuseppe Cocco, *A Nova Qualidade do Trabalho na Era da Informação*, *in* Informação e Globalização na Era do Conhecimento, 262, 275 (Helena Maria Martins Lastres &, Sarita Albagli eds., 1999) ("Power is rapidly moving towards sharper hierarchies in the international division of knowledge ownership—ownership of the raw materials, the production cost of which increasingly determines the relative price of goods and services that are exchanged internationally. From now on, copyrights, trademarks and trade secrets will be the actual subject of international negotiations.").

286. *See generally* Dorine Verheij, Jouke Tegelaar & Nick Campuzano, *Asset segregation: Its many faces and challenges faced*, leidenlawblog (Mar. 22, 2019) https://leidenlawblog.nl/articles/asset-segregation-its-many-faces-and-challenges-faced [https://perma.cc/QL9B-Z7CQ] (for an elementary introduction to this concept).

287. U.N. Comm'n on Int'l Trade Law, Report of Working Group I (MSMEs)

horizontal exchange of workforce, goods, capital, and assets generally, along the lines of a more stringent contractual interdependence and interliability, but without reaching the level of progressive subincorporations. Relevantly for the present study,

> SMEs can share existing technology provided by one or more platform members, directly co-produce new technology within the platform itself or acquire technology licensed/transferred by subjects that are not party to the platform. Network contracts may also ease the *provision of technical assistance given to SMEs related to intellectual property by business and government bodies*, by facilitating the transfer of information and knowledge to a single collective subject and its subsequent dissemination among the network members.[288]

As far as trade secrets are concerned, the fact that these networks would need to "generate strong safeguards against knowledge leaking outside the network"[289] is a due observation; however, it also entails that the members of a network would need to be ready to level their cybersecurity standards, as to make the project workable and avoid placing the whole network at risk. General cyber-hygiene standards would need to be homogenized within the network, and the actual "carrier" of the trade secret would need to be kept monitored as it faces the network as its "liability multiplier." Mutual recognition and enforcement and legal standing in all "jurisdictions of operation" should be granted only after a meticulous inspection on the effective comparability of cybersecurity standards put in place by all network hubs.

IX. From Private Contracts to Public International Lawmaking

Moving away from private international law and entering the realm of its public side, the failure of international law practice and scholarship to systematically address the economic and noneconomic losses of confidential information following cyberespionage intrusions leaves one dismayed.[290] The first background concern is "whether the cyber-attack should be treated as a law enforcement matter or a national security matter. Relevant to this determination is whether the level of force used in the cyber-attack rises to that of an armed attack."[291] Eminent scholars

---

On the Work of its Twenty-Eighth Session, U.N. Doc. A/CN.9/900 at 2 (May 19, 2017), https://undocs.org/en/a/cn.9/900 [hereinafter Comm'n on Int'l Trade Law].

288. *Id*. at [para.II(4)18] (emphasis added).

289. *Id*. at [para.III(3)30].

290. *See* Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 Colum. J. Transnat'l L. 275, 295 (2013).

291. Michael Gervais, *Cyber Attacks and the Laws of War*, 30 Berkeley J. Int'l L. 525, 544 (2012); *see* Greg Austin, *Middle Powers and Cyber-Enabled War: The Imperative of Collective Security*, in Securing Cyberspace: Int'l and Asian Perspectives 23, 37 *(*Cherian Samuel & Munish Sharma eds., 2016) (discussing how Russia and China committed to shield each other's trade secrets from cyber-enabled exploitation).

have recently engaged in lengthy discussions on this node, so that there is no necessity to restate the doctrinal hurdles here.

This Article is rather concerned with another public international law aspect which to be examined, requires a change of paradigm: what if a State is *not* responsible for or complicit in cyberattacks, but rather negligent in letting this happen from within the borders of its territorial sovereignty, or by its officers? There is literature on this standpoint just as much; however, the salient question here is whether trade secrets thefts may reach the threshold of armed attack, not simply because of the way they are executed, but for the IP assets (perhaps pertaining to the military or the intelligence) it steals. This last action is in fact perilous for the economy of all countries, yet might threaten the survival itself of smaller economies, up to jeopardizing the preservation of the social order in those States which show already weak economic performance indicators and strongly rely on trade secrets and public-private partnerships throughout their state security chain. When the trade secret is necessary for the defense industry of countries tied together in a mutual defense mechanism in the form of a multilateral treaty, the state responsibility of the negligent State may arise not only for the negligence per se, but for the breach of said treaty as well. In order to avoid such consequences, the State should at least demonstrate to have enacted stringent laws in due time,[292] and to have actively enforced them within the limits of its financial and bureaucratic resources, whilst also cooperating with other States.[293] Shielding responsibility this way is even more important in today's globalized world, where "[r]elations between States are often so dense that a broad and rigorous rule on complicity would require constant scrutiny by States on whether their conduct which is prima facie 'neutral' does not stray into 'complicity'".[294] When it came to the International Law Commission (ILC) Draft Articles on Responsibility of States for Internationally

292. *E.g.*, Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, Supplementing the 2000 United Nations Convention Against Transnational Organized Crime, art. 11(a), May 31 2001, 2326 U.N.T.S. ("In an effort to detect, prevent and eliminate *the theft*, loss or diversion of, as well as the illicit manufacturing of and trafficking in, firearms, their parts and components and ammunition, each State Party shall *take appropriate measures [. . . t]o require* the security of firearms, their parts and components and ammunition *at the time of manufacture*, import, export and transit through its territory.") (emphases added).

293. *See generally* Stolen Asset Recovery Initiative and U.N. Convention Against Corruption, October 31, 2003, 2369 U.N.T.S. 6 (emphasis added) (displaying an international community "[d]etermined to prevent, detect and deter in a more effective manner international transfers of *illicitly acquired assets* and to strengthen international cooperation in asset recovery"). Even more relevant to the specificity of IP assets is the 2011 Anti-Counterfeiting Trade Agreement, not yet entered into force; on its potential and shortcomings respectively, see Andrew F. Popper, *More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership*, 12 Nw. J. Tech. & Intell. Prop. 253, 280 (2014); Luciano Floridi, *The anti-counterfeiting trade agreement: The ethical analysis of a failure, and its lessons*, 17 Ethics and Information Tech. 165 (2015).

294. Georg Nolte & Helmut Philipp Aust, *Equivocal Helpers—Complicit States, Mixed Messages and International Law*, 58 Internat'l & Comp. L. Q. 1, 2 (2009).

Wrongful Acts (ARSIWA), China criticized the provision of a Draft Article on state complicity, but adopted an ambivalent stance by not opposing in principle its inclusion in the project, as if it was not yet ready in practice whilst normatively willing to take that path.[295] Japan generally agreed with the Commission, demanding just a few clarifications on the elements to assess state intent in assisting other countries to commit an internationally wrongful act.[296] The position of Australia can be extrapolated by analogy: in its interpretative declaration attached to the meaning of "to assist" in Art. 1.1.c of the Ottawa Convention, Australia interpreted that expression to mean "actual and direct physical participation" but not "indirect security support" to nonparties to that Convention.[297]

The dynamics of attribution, (co-)responsibility, retaliation, complicity, negligence and so forth are not all those of relevance: geopolitical dynamics may come to bear legal poignancy; among them, the Global North/Sud divide in its interconnections with the "right to development." If a GN country steals assets protected as trade secrets from a GS country, should that country's classification as a GN country be factored in as an aggravating circumstance for the appraisal of its internationally wrongful act? On parallel lines, should a GS country's responsibility be mitigated or extenuated when its stealing occurs at the expense of a GN country? Arguably, the first scenario sounds more acceptable than the latter. The fact that "quasi-developed" countries like China keep explicitly linking the security of their cyberspace to their (legal) right to development[298] is

295. U.N. GAOR, 54th Sess., 22d mtg. at 11, U.N. Doc. A/C.6/54/SR.22 (Nov. 1, 1999) ("Chapter IV of the draft, dealing with the implication of a State in the internationally wrongful act of another State, included article 27 (Assistance or direction to another State to commit an internationally wrongful act) and article 28 (Responsibility of a State for coercion of another State), which in his opinion contained some ambiguities. The words "directs and controls" and "coercion" were not identical in meaning; in addition those three concepts shared some aspects of the meaning of "aids or assists". He therefore agreed with the Commission's decision to redraft the two articles in three distinct articles. The new title for chapter IV of the draft (Responsibility of a State for the acts of another State) was more appropriate than the original title. He nevertheless felt that the title should also contain the notion of wrongfulness."). Then, eight years later, the Chinese Government reiterated his strong support in favour of a general rule of nonassistance in wrongful acts in international law, regardless of their gravity. *See* Ma Xinmin, *Statement by Mr* Ma *Xinmin, Chinese Delegate, at the Sixth Committee of the 62*nd *Session of the UN General Assembly, on Item 78 "Responsibility of States for Internationally Wrongful Acts"*, Permanent Mission of the People's Rep. of China to the UN (October 23, 2007), http://www.china-un.org/eng/xw/t375208.htm [https://perma.cc/ABA5-3WEV] (emphasis added) ("*All* international wrongful acts should not be recognized or rendered assistance to. All States have the obligation to cooperate in order to bring an end to these acts.").

296. Int'l Law Comm'n, Report on the Work of its Fifty-First Session, U.N. Doc A/CN.4/492, at 107 (1999).

297. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, Mar. 11, 1999, 2056 U.N.T.S. 211.

298. Riccardo Vecellio Segate, *Fragmenting Cybersecurity Norms Through the Language(s) of Subalternity: India in "the East" and the Global Community*, 32

noteworthy. One consideration might seem to disprove the above: most scholars posit that developing countries are "generally better off with a lax IP system that allows for certain forms of imitation and technological learning."[299] For example, "[w]hen the United States was still a relatively young and developing country, . . . it refused to respect international intellectual property rights on the grounds that it was freely entitled to foreign works to further its social and economic development."[300] However, this widely-held theory[301] might be valid *internally* as to foster technology diffusion, whereas international thefts of these countries' IP wealth are certainly not beneficial to their economic systems and growth. Another counterargument is that most of such literature is IP-generic rather than trade secret–specific.

Conclusions: Best Practices and Policy Recommendations

This study has adopted an international legal and macroeconomic approach to its proposed topic, arguing that in order not to disperse the actual and potential value of trade secrets, a reconceptualization of the latter in public-good terms is urgently warranted. Limited to what stands as relevant to its political economy manifesto, it has thoroughly demonstrated that, considering how . . .

- After a few decades of declining interest,[302] trade secrets are increasingly regaining momentum for businesses, especially in the aftermath of the financial crisis[303] (as they are cheaper and

Colum. J. Asian L. 78, 108 (2019).

299. Xuan Li & and Carlos Maria Correa, Intellectual Property Enforcement: International Perspectives 55 (2009); *see* James Gathii & Cynthia Ho, *Regime Shifting of IP Lawmaking and Enforcement from the WTO to the International Investment Regime*, 18 Minn. J. L., Sci. & Tech. 427, 436–437 n.31 (2017) ("TRIPS reflects a compromise between the proposed strong IP protection advocated by the United States versus much weaker IP protection advocated by India.").

300. US Congress Office of Tech. Assessment, OTACIT-302, Intellectual Property Rights in an Age of Electronics and Information 228 (1986).

301. Debora Halbert, *Piracy, Open Source, and International Intellectual Property Law*, *in* Asia.com: Asia Encounters the Internet 97, 102 (K.C. Ho, Randolph Kluver & Kenneth C.C. Yang eds., 2003); Sourav Chatterjee, Jesse David, Fei Deng, Christian Dippon & Mario Lopez, *Worldwide: Intellectual Property Rights in Developing Nations*, Mondaq (March 4, 2008), http://www.mondaq.com/unitedstates/x/57856/Trademark/Intellectual+Property+ Rights+In+Developing+Nations [https://perma.cc/9VB2-HSA4].

302. Dobrusin, *supra* note 28, at 324–325; *see* Susan K. Sell, Private Power, Public Law: The Globalization of Intellectual Property Rights 66–67 (2003) ("Since patents were frequently held to be invalid and infringers faced low penalties that usually amounted to payment of a royalty, US businesses sought other means of protection from competition, such as trade secret protection [and] *government subsidies combined with high secrecy* levels (in defense industries). . . . In fact, by the late 1960s Japan came to dominate the global consumer electronics market. The lax U.S. domestic patent environment began to change in 1980 and the Supreme Court signaled a new attitude toward patents.") (emphasis added).

303. *See*, *e.g.*, Brandon Kinnard, *Keep It Secret; Keep It Safe: A Practitioner's Guide To The "BRIC" Trade Secret Regimes*, 3 Am. U. Bus. L. Rev. 503–517 (2014).

"faster" than other forms of IP such as patents) and across all industries and company sizes.

- Given their average economic and intelligence value, they are equally important as targets of industrial and military espionage executed via the endless loopholes offered by the cyberspace, exemplified by mutual accusations between the US and China, against a background of dual-use technologies and general blurring of civilian/military distinctions coalescing in an inappropriate "war language."
- SMEs particularly benefit from an effective and smarter trade secrets protection, and start-up-led innovation is a policy goal pursued by most economic ecosystems, particularly so in emerging markets. Western countries should note the resolute (someone might say "aggressive") way China asserts the protection of its assets domestically and internationally.
- Trade secrets can be reconceptualized as public goods, both innovation-wise and security-wise, and the costs of their theft can be read as undue geo-economic losses or—worse—transfers of (informational) wealth shifting the burden to the social body, with particular reference to those categories of taxpayers that, neither shareholders nor *formal* stakeholders, de facto support specific collective programs for innovation.
- Yet, even major multinational corporations benefit from protecting trade secrets, especially when the latter overlap with state secrets in the production operated by hybrid civilian/military corporations (the oligopolist—quasi-monopolist in their respective geographical markets—Airbus and Boeing represent this hybridity to its best).
- A company whose trade secrets have been breached once, is unlikely to be considered trustworthy by market players, buyers, and potential partners, even in the future, and particularly so when economic cycles shorten their curve span,[304] to the extent that missing a cycle equates to being pushed at the margins of the market.
- Trade secrets are the only IP protection system based on the paradigm of *exclusion by secrecy* rather than *exclusion by*

304. *Catch the wave: The long cycles of industrial innovation are becoming shorter*, The Economist (Aug. 11, 2014), https://www.economist.com/special-report/2014/08/11/catch-the-wave [https://perma.cc/3RRC-9RA6]; *but c.f.* Leonardo Burlamaqui, *Creative Destruction as a Radical Departure: A New Paradigm for Analysing Capitalism*, *in* Schumpeter's Capitalism, Socialism and Democracy: A Twenty-First Century Agenda 21, 45 (Leonardo Burlamaqui & Rainer Kattel, eds., 2018) (stating that "economic waves" and "economic cycles" might not be interchangeable terms from a Schumpeterian perspective where "development unfolds in *waves*, cumulative industrial revolutions that rejuvenate the economic landscape, which implies fluctuations in economic activity but not regular, recurring, or multiple cycles.").

publicity,[305] as well as on the paradigm of (potentially) unlimited exploitation in time rather than expiration (contrast it with, e.g., patents, whose licensing can also be compelled by law[306] in most jurisdictions).

- Yet, most legal systems address them traditionally (i.e. with a property or liability vocabulary) in court proceedings, just like any other IP right whose disclosure is not only unproblematic, but even required by law.
- The above is so important that as soon as a trade secret is no longer secret, there is little to protect anymore, and its patentability is almost impossible to prevent in court.[307]
- Judicial measures are nonoptimal, as they come too late, too narrow in scope, exception-filled, time-limited, frustrated with officials' corruption, and unable to compensate the entrepreneurial loss up to its true market *and societal* value.
- Such judicial measures are overburdened with evidentiary challenges, including: attribution in the cyberspace, evidence thresholds, disclosure requirements,[308] and deceiving claims related thereto. Disclosure requirements are extremely burdensome when it comes to cyber-enabled thefts of trade secrets (or to thefts of trade secrets stored in the cyberspace), because the advent of the cyberspace changed the *foundational ontology* of trade secret

305. Even copyrights, which are neither *granted* nor necessarily *made public* by the State in a listing, need somehow to be known in order for relevant third parties to recognize them and enforce their protection.

306. *See* Abbe E. L. Brown, Intellectual Property, Human Rights and Competition: Access to Essential Innovation and Technology, 8 n.18 (2012) for examples of "compulsory licensing" under the TRIPS regime within Brown's sources.

307. Meaning that once a trade secret is stolen from company 1 by company 2, and *exactly because* since that point onwards it is no longer a trade secret of that company 1 unless it enters a joint-venture with company 2 by "mutualizing" the secret, the stolen material/idea becomes either a trade secret of company 2 (and this is even questionable, because company 1 would arguably still "know" it) or, almost always, finds its way towards patenting by companies 3, 4, 5 etc. (which might even have informal ties or agreements with company 2). Indeed, *especially when companies 1 and 2 belong to different jurisdictions*, a claim of theft does not constitute a bar to filing a patent request: first, because once an information is no longer secret, it enters the public domain and may "accidentally reach" those companies 3, 4, 5 etc.; second, as the filing itself of a patent does not compel any detailed disclosure to the general public beyond the patent office's evaluators. The reader is advised to note that this general mechanism might differ slightly jurisdiction to jurisdiction, yet it remains overall true in its core substance. Moreover, the reader is warned that the mechanism described here is not related to the one known in common-law jurisdictions as "patent prosecution bar;" *see*, *e.g.*, Christopher C. Funk, *The Bar Against Patenting Others' Secrets*, 19 Stan. Tech. L. Rev. 239–292 (2016).

308. Catherine L. Fisk, *Taking the Long View on Competition and the Mobile Employee: Lessons from the United States History of Efforts to Regulate Employee Innovation and the Mobility of Workplace Knowledge*, *in* Business Innovation and the Law: Perspectives from Intellectual Property, Labour, Competition and Corporate Law 214, 221 (Marilyn Pittard, Ann L. Monotti & John Duns eds., 2013).

thefts, so radically that in most cases one should speak of *illegal copy* rather than *stealing*. The secret is unlawfully copied and misappropriated, yet the original owner is not necessarily deprived of it completely (only of its commercial exploitability). One of the consequences is that when facing disclosure requirements in court, the allegedly violated party has still something to lose, thus it cannot disclose thought-free as it would have done if the secret was entirely out of their hands; also, copies cannot be easily proven, and even companies themselves can rarely ascertain they actually occurred. This way, frauds against trade secret owners are perpetrated whenever the latter, to avoid disclosure requirements in courts, decide to settle extrajudicially thus paying for acquiring legal assurances that a supposedly *stolen* trade secret (which might have actually never been even *copied*) would be destroyed or not used. In all senses, copies are harder to address when compared to proper full deprivations antecedent to the cyberspace; this holds true both before and outside the courtroom. The complexity of such multifaceted conceptualization compels an overall change of legal mindset, translating concretely into a shift from *ex post* (injunctions, compensations) to *ex ante* (compulsory multilayered cyber-hygiene, cybersecurity clauses in know-how sole/exclusive licensing agreements, homogeneous cybersecurity standards in networked digital supply chains) legal solutions, updated enough to cater for the attack-one-defend-all multispot cyberattack dynamics of a highly interconnected economy. This is to be applied while remaining mindful of potential chilling effects, and vigilant about possible over-bureaucratization. This "compulsory cybersecurity" approach prevents rather than trying to redress, thus levelling the existing differences before the law between external thefts of trade secrets and misappropriations performed by still-on-contract employees. Higher corporate costs due to cyber-requirements implementation ought to be expected; however, the "soft" expenses for ICT preparedness are to be preferred over the "hard" ones which are necessary in ICT recovery scenarios, when insurances may compensate economically yet would never restore the business itself. What is more, defensive strategies might be incentivised by the State (directly, through subsidiarization, or indirectly, by virtue of fiscal relaxation).

- Trade secret protection is increasingly assigned a specific piece of legislation, or section within the law of tort, confidentiality, fair competition, etc.
- Wherever it is ultimately located within the sources of a legal system, trade secret law can be either directly updated, or left as it stands but indirectly complemented by binding cybersecurity and criminal laws underpinned by alternative rationales and able to "fill the gaps" in trade secrets protection as a collective

good for security, sustainability, development, and in the gravest cases, the survival itself of a whole economy.

- Trade secrets frameworks already include a prevention requirement, thus it is only a matter of checking that it is more grounded and harder to satisfy, as well as complied with *beforehand*, by further defining it and equipping it against cybersecurity threats, with an eye on the public meaning and international implications of a trade secret, as much as on the changing threats landscape.
- Cybersecurity measures are not desirable to the same extent in closed and open economic systems, with due regard to offsetting the harmful effect of hyper-regulation (Internet policing; "surveillance capitalism";[309] inconvenience to protect intellectual property via trade secrets) with the added value of a trade secret in a specific market. For the purpose of this analysis, "closed" economic systems are domestic ones, or highly integrated economic areas such as the EU's single market; "open" ones are international (especially between geopolitically competing powers).
- The Schumpeterian "knowledge spill-over" theory of entrepreneurship predicted that innovating territories are built on innovation clusters and hubs which are severely jeopardized by the withdrawal of an innovative asset, well beyond the actual, immediate, local impact of such a withdrawal and its mere business quantification.
- The same Author clarified how it is innovation, not capital or labour, that triggers the creative destructions necessary for capitalist systems to constantly renovate themselves.
- The Schumpeterian model of entrepreneurial competition can find application as to theorize that from a nonindividual perspective, domestic thefts are only moderately harmful to a closed innovation system, insofar as they only call for joint ventures or the overcoming of adaptability gaps in terms of time and operability.
- Acting as creative destructors in a Schumpeterian sense, trade secret thefts offset the arguments brought forward by the mentioned two theories elaborated by the same author, so that one can theorize, as a final result, that trade secrets thefts are domestically neutral (through purely macroeconomic lenses).
- States might be held internationally responsible for failing to protect trade secret-based investments within their territories, in accordance with relevant BITs.
- Enforcing injunctions and compensation orders abroad presents almost insurmountable challenges (related to jurisdiction, investigation, and evidence), not to mention how integrated most markets are in the world economy, through tangles of globalized supply chains and so-called "networked contracts".

309. *See generally* Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier (2019).

- The domestic "entrepreneurial incentive" recognized by judges as "opportunity/cost" can be deemed to bear a nationwide facet, meaning that States invest only insofar as they anticipate economic (and reputational) reward.
- . . . each State of the international community should:
- Make sure companies implement and meet reasonable, progressive and tailored-to-business cyber-hygiene and cyber-risk-management-cycle*** policies and standards (by enforcing them nationally).
- Legislate on the justiciability (and justifiability) of storing trade secrets without proper[310] cyber-hygiene: on the tort side, charged vis-à-vis all those who hold direct and indirect interests in the preservations of such secrets, and on the criminal side (in the gravest occurrences), prosecuted as contempt of State; indeed, the latter scenario can be deemed equivalent to a leak of military secrets to foreign powers (one might think of a high-tech IT startup programming dual-use surveillance software, whose coding is almost always protected as trade secret).
- Sort trade-secret-owner companies in different categories, related to their risk exposure to threats and misappropriation, on the model of Mainland China's cybersecurity laws.
- Criminalize trade secrets stealing, following the choice of the US legislator.
- Perform in-depth market and policy research on the best way to tailor mandatory cybersecurity measures to the different capacities and needs of companies, distinguishing between private and state-owned, sensitive or irrelevant for security and public order, national or multinational, small or big, innovative or traditional.
- Take note of the Pacific region as the one offering some of the best and worst examples of trade secrets protection. When keeping the United States as a benchmark, China's multilayered cybersecurity law (incidentally) offers higher and effective protection to this form of intellectual property, whilst surrounding countries adopt too liberal and deregulated a stance, which does not differentiate among different companies' products/reach and does not contemplate binding preventive actions and/or the criminalization of thieves.

***Cyber-hygiene, customized to the purposes of protecting trade secrets, should include proportionally and progressively the (technical

310. This "appropriateness" might prove difficult to define legally. The criterion to be applied can be that of a percentage of the company's yearly income to be invested in cybersecurity, following a self-assessment of all variables including the extent of previous provision of financial means (e.g. incentives by the State), the subject-matter of those secrets, the overall conditions of the company and expertise of its managers, etc. Any criterion should be both defined and applied with reasonable care, good faith and genuineness, according to detailed previously-elaborated scales.

and behavioral,[311] physical and legal[312]) measures included in the table below.[313] Said table sorts the suggested measures into two categories, subject to different implementation *ratione materiae et ratione loci*. The essential ones should be compulsory for both low-exposed and high-exposed companies, yet even companies deemed at low risk should adopt the nonessential ones in order to claim in court that they "reasonably protected" their trade-secret assets; however, this last decision is left to private choice. The second column features less urgent and/or fundamental measures, to be considered binding only on companies listed by the State as pivotal for the national economy, or as carrying sensitive data protected as trade secrets; thought should also be given to the companies' likelihood of falling victim to cyber-enabled thefts: when grounds stand for such a likelihood, companies would better be required by law to implement both categories of measures indicated in the table to follow.

311. *See* Ralph Foorthuis, Tactics for Internal Compliance: A Literature Review 163–164 (2012) (Ph.D. thesis, Utrecht University) ("To prevent unethical business conduct and avoid regulatory penalties and loss of reputation, compliance management includes implementing *structures and processes* . . . . As one tactic is typically not sufficient to obtain compliance, multiple tactics need to be combined into a coherent strategy.") (emphasis added).

312. The Italian jurisprudence on trade secrets is enlightening about this combination; *see*, *e.g*, Francesco Banterle, *The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis*, *in* Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? 411, 418–421 (Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt & Gintarė Surblytė-Namavičienė eds., 2018).

313. Some measures have been retrieved from the following publications: Gregory J. Touhill & , C. J. Touhill, Cybersecurity for Executives: A Practical Guide (2014); *Advancing Cyber Resilience Principles and Tools for Boards*, World Economic Forum (Jan. 2017), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files / Adv_Cyber_Resilience_Principles-Tools.pdf.pdf [https://perma.cc/MU3W-ZVPY]; Scott Rosenberg, *Firewalls Don't Stop Hackers. AI Might.*, Wired (Sep. 27, 2017), https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might [https://perma.cc/M5CD-2SM7]; Derek P. Martin, *An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation*, BYU L. Rev. 949–981 (1993); Andy Jones & Debi Ashenden, Risk Management for Computer Security: Protecting Your Network and Information Assets (2005); Bhavani M. Thuraisingham, Database and Applications Security: Integrating Information Security and Data Management (2005); Syngress, Securing Intellectual Property: Protecting Trade Secrets and Other Information Assets (2009); Computer and Information Security Handbook (John R. Vacca ed., 3d ed. 2017).

Security Steps To Be Taken Before Discovery Of A Breach {Planning, Prevention, Protection And Monitoring}		*Security Steps To Be Taken Upon Detection Of A Serious Breach {Technical Response, Business Continuity And Incident Recovery}*
Essential	• Drafting a comprehensive incident response and business continuity plan. • Ensuring the safety of physical environments. • Implementing a clean-desk policy. • Identifying internal and external threats (SWOT analysis). • Introducing risk prevention, identification, assessment, mitigation, monitoring and reporting protocols; performing an expert complete preventative IT-exposure prophylaxis. • Complying with relevant international quality standards (e.g. Cybersecurity Standard ISO/IEC 27001, NIST Cybersecurity Framework, ENISA Cybersecurity Standard) and protocols. • Documenting the definition and frequent revision of personnel cybersecurity responsibilities (especially with the appointment of a CISO and a team of risk managers), including computer-access policy complemented by fingerprinting et similia. • Requiring suppliers, partners, consultants, attorneys, auditors, outsourcers, data handlers, technicians, etc. to sign and individually well understand nondisclosure agreements[314] (including a confidentiality clause and a non-subtransfer clause). • Introducing nonreplication policies mandating the prohibition to store trade secrets on nonregistered and/or personal mobile/nonmobile devices. • Specifying that employees should not rely on expectations of privacy, as far as company devices and services (e.g. corporate email account) are concerned. • Compartmentalizing password/access management encryption of critical business assets, as for preventing both internal thefts and external undue usage. • Blocking USB connections during lunchtime and generally during unsupervised breaks. • Simultaneously distributing trade secrets and segmenting their memory networks (but to an extent only, as per not causing the opposite problem of exaggeratedly uncontrollable dispersion, which stands as an insecurity multiplier). • Keeping all (antivirus, antimalware, firewalls, VPNs, etc.) software updated to the most recent patches.	• Collecting and preserving evidence. • Disclosing the breach to affected individuals, the insurer, and public authorities, and reporting its operational followup. • Complying with (legal and ethical) data privacy and breach notification requirements on elements that might have affected third parties (privacy-endangering externalities). • Determining (estimating and then quantifying) the loss, and sharing the information with all "interested parties"

314. *But see* Villasenor, *supra* note 56, at 348–349 (explaining as to why no overconfidence should be attributed to these agreements "[i]f a company's trade secrets are compromised in a cyberintrusion targeting a third party to whom those secrets have been disclosed, an NDA may be of little use. Although NDAs generally require third-party recipients to exercise at least a reasonable degree of care in protecting information, a sufficiently sophisticated intrusion might circumvent even very strong security measures, giving the third-party grounds to assert that it honored the NDA despite the compromise. Not to mention, *arguing about responsibility for a breach does nothing to recover the lost information*.") (emphasis added).

Security Steps To Be Taken Before Discovery Of A Breach {Planning, Prevention, Protection And Monitoring}		*Security Steps To Be Taken Upon Detection Of A Serious Breach {Technical Response, Business Continuity And Incident Recovery}*
Less Urgent	• Contracting a digital forensics team. • Regularly reviewing all corporate operational regulations and techniques, as to ensure their continued effectiveness and adaptation to changing market conditions and security environments. • Introducing competitor benchmarking tests (e.g. on risk appetite and risk tolerance limits), best-practice adaptation tests, stress tests, and scenario reaction test. • Establishing a customer private key storage policy. • Establishing clear guidelines on employees' use of corporate intranet, corporate email, public Wi-Fi networks, private social media profiles, personal devices at home and at work, etc. for the overall purpose of avoiding "cross-contamination" (one might think of a parallel with the "cold chain" and "hot chain" in the food industry) between "internal" and "external" as well as "public" and "private" or "secured" and "unprotected". • Requiring employees to subscribe to preplanned offboarding procedures and to sign in advance an Employer Property Return Agreement. • When data disclosure to third parties is unavoidable, performing a need-to-know analysis to understand how to redact to-be-shared versions of internal documents. • Designing algorithms in a modular manner as to facilitate their partitioned storage. • Formalizing an "Ethics and Security Hotline" or (as a minimum) a 24/7 dedicated email account. • Setting up an insurance plan, keeping in mind exclusionary policies and premium costs. • Establishing an online *and offline* routine system of periodic security-check reminders. • Liaising with external/institutional incident-response teams (e.g. the CSIRT communities in Europe, or US-CERT in the United States). • Asking for and considering the views of private and public cybersecurity rating agencies. • Raising cybercrime awareness (e.g. on phishing or social-engineering hacking techniques) among *all* employees by providing them with paid training, along with professional development courses for *key* employees,[315] on a regular basis. • Storing "negative information"[316] in uneasy-to-access locations. • Identifying client private keys to be held in cold cloud storage systems, and related insurance scheme. • Limiting cloud storage to what strictly necessary, as to limiting the chance of being targeted by cloud-based attacks. • Screening employees on entry[317] and especially on leave.[318] • Implementing schemes for avoiding allegations of misappropriation, including disclosure of post-employment obligations for incoming professionals and adequate screening of their former job posts (especially when the previous firm is a direct competitor in that relevant market). • Securing feasible "preventive procurement" arrangements, whereby the company ensures that its possible need for sophisticated software/hardware enhancement is satisfied in time, especially in the event of security emergency and business disruption.	• Correctly managing crisis communication, including social media. • "Transferring assets between wallets" and reassigning competences. • Post-factum information security auditing. • Pressing charges against the thieves (in the rare event they are known) and recovering what possible. • Reactivating the process of market differentiation by modifying "just enough" the stolen secret as to retain competitive advantage, and placing this new secret under improved security conditions. • Opting for intelligence sharing on cyberattacks with similar corporations and organizations.

315. In this case, they are the central/division managements, additionally to those who *know* the secret, those who *can know* it (i.e. have access to it in different situations, for different reasons, and to variable extents), along with all personnel involved in the security and maintenance of the IT infrastructure of the company. When secrets are particularly valuable, the awareness of their details is usually fragmented and distributed so meticulously that no one actually has the keys to the whole picture; in some industries and production lines, however, this might not be technically feasible, logistically convenient, or cost-effective.

316. Pedraza-Fariña, *supra* note 182, at n.105 (quoting Eric von Hippel, *Cooperation Between Rivals; Informal Know-How Trading*, 16 Res. Pol. 291 (1987) (defining negative information as "knowledge about what does *not* work to solve a problem").

317. Whilst paying attention to the limits imposed by the law; *e.g.*, Invest Japan Dept., *Laws & Regulations on Setting Up Business in Japan*, JETRO 66 (Jun. 2016), http://www.invest-japan.go.jp/committee/simplify_wg_02/shiryo_05–2.pdf [https://perma.cc/CU62-3LX6] ("[In Japan,] both the disclosure of former employers' trade secrets by workers and questioning by enterprises of workers about such trade secrets are prohibited by law under the Unfair Competition Prevention Act.").

318. Dobrusin, *supra* note 28, at 322–323.