# Vulnerabilities, Cybersecurity, and the Role of Law and Regulation herein

# Kwetsbaarheden, cyberveiligheid en de rol van wet- en regelgeving hierin

Proefschrift ter verkrijging van de graad van doctor aan de
Erasmus Universiteit Rotterdam op gezag van
de rector magnificus
Prof.dr. A.L. Bredenoord
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op
donderdag 11 november 2021 om 10:30 uur

Jian Jiang
Shanghai, China

Erasmus University Rotterdam

**Promotiecommissie**

| | |
|---|---|
| Promotoren: | Prof. dr. N.J. Philipsen |
| | Prof. dr. E. Salzberger |
| Overige leden: | Prof. dr. M.G. Faure LL.M. |
| | Prof. dr. E. Carbonara |
| | Prof. dr. R. Sarel |

This thesis was written as part of the European Doctorate in Law and Economics programme


An international collaboration between the Universities of Bologna, Haifa, Hamburg and Rotterdam.
As part of this programme, the thesis has been submitted to the Universities of Bologna, Haifa, Hamburg and Rotterdam to obtain a doctoral degree.




In memory of Prof. Dr. Manfred Neumann (1933–2016)

# Preface and Acknowledgments

This thesis originates from my observations about the important role played by software vulnerabilities in the increasing number of cyberattacks globally. Nowadays, it is not difficult to conjure up images of hacked power plants, remote-hijacked public transportation systems, etc. Shortly before the completion of this thesis, one of the United States' largest oil pipelines, Colonial Pipeline, was hacked and forced to pay the hackers a ransom of nearly $5 million, according to the Wall Street Journal. By exploiting hidden vulnerabilities, hackers are plundering business secrets, stealing digital consumer records, and trying to reshape the world quietly.

Most of society lacks awareness of software vulnerabilities. Software vendors seem unlikely to discuss flaws in their products publicly, and the related markets of vulnerabilities are often opaque. My thesis tries to introduce to the readers a structured discussion and analysis of software vulnerabilities vis-à-vis the challenges of cyberattacks. I hope that my research will stimulate more contributions to this topic.

It has been a huge challenge to complete this thesis. The ongoing crises of COVID-19 has increased difficulties of my research work. It is with the support and assistance from many people that it has been possible to complete my thesis.

First and foremost, I would like to thank my supervisors, Prof. Dr. Niels Philipsen and Prof. Dr. Eli Salzberger, without whom my research would not have been possible. It is their creative insights, motivating guidance, inspiring advice, and patient help that led me to complete my research project. They guided me to organically incorporate economic analysis with legal theory and made a vital contribution to my thesis.

I am deeply indebted and wholeheartedly grateful to Prof. Dr. Michael Faure for his never-ending support, immense encouragement, and enlightening comments on the earlier drafts of my thesis. I wish to acknowledge Prof. Dr. Michael Faure's understanding and suggestions, which helped me to keep going.

I would also like to take this opportunity to express my gratitude to Prof. Dr. Alan Miller.

I am thankful for his support when I was developing my research ideas and economic models, as well as his trust in me on my academic journey. Alan contributed significantly to my thesis.

Special thanks must go to Prof. Dr. Jonathan Klick and Prof. Dr. Jarek Kantorowicz. The discussions with Prof. Dr. Jonathan Klick sharpened the econometric part of my research. The valuable ideas and insights in their lectures greatly improved my empirical work. Special thanks also go to Prof. Dr. Francesco Parisi, who gave my research project significant recognition and encouragement.

Parts of my thesis were presented at various conferences, among which were the EDLE conferences in Rotterdam, Bologna, and Hamburg, as well as the colloquium at the Cyber Centre at the University of Haifa. I would like to express my special gratitude to Prof. Dr. Kees van Noortwijk, Prof. Dr. Franziska Weber, Prof. Dr. Louis T. Visscher, Prof. Dr. Sharon Oded, Prof. Dr. Niva Elkin-Koren, Prof. Dr. Todd Kaplan, and Prof. Dr. Luigi Franzoni.

I would like to present my great appreciation to my colleagues in Rotterdam and Haifa, especially Marianne Breijer, Prof. Dr. Elena Kantorowicz-Reznichenko, Yulia Lischinsky, and Dr. Michal Ben-Gal. Their patience and supportive work have always been there for me. Sincere thanks go to all the members in the reading committee of my thesis, for their valuable time and remarks. They are Prof. Dr. Michael Faure, Prof. Dr. Emanuela Carbonara, and Prof. Dr. Roee Sarel.

I am expressing my heartfelt gratitude to Prof. Dr. Justus Haucap, Prof. Dr. Christian Koenig, Dr. Karni Chagal and Dr. Shu Li, for their constant support for me. Prof. Dr. Hans-Theo Normann also deserve special recognition for his encouraging comments on my empirical work in the thesis.

Finally, I wish to thank all my family members and friends, for accompanying me on this long journey and endorsing me with unconditional love.

# Contents

## List of Tables

**List of Figures**

**References**


Ablon, Lillian; Libicki, Martin; Golay, Andrea (2014), Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, *RAND CORPORATION (Mar. 2014),* Retrieved on 20 November 2020, from http://www.rand.org/pubs/research_reports/RR610.html

Ablon, Lillian; Bogart, Andy (2017), Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, *RAND Corporation,* Santa Monica, CA, p. xii., Retrieved on 20 November 2020, from www.rand.org/t/RR1751

Aitel, Dave; Tait, Matt (2016), Everything You Know About the Vulnerability Equities Process Is Wrong, *Lawfare,* Aug 18, 2016, Retrieved on 20 November 2020, from https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong

Albright, David; Brannan, Paul; Walrond, Christina (2010), Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment, *ISIS (Institute for Science and International Security) Report,* Retrieved on 20 November 2020, from https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Algarni, Abdullah; Malaiya Yashwant (2014), Software Vulnerability Markets: Discoverers and Buyers, *World Academy of Science, Engineering and Technology, International Journal of Computer, Information Science and Engineering,* Vol. 8, No. 3, pp. 480-490

Alheit, K. (2001), The applicability of the EU Product Liability Directive to software, *The Comparative and International Law Journal of Southern Africa*, Vol. 34, No. 2, pp. 188-209

Allodi, Luca; Shim, Woohyun; Massacci, Fabio (2013): Quantitative assessment of risk reduction with cybercrime black market monitoring, *Security and Privacy Workshops (SPW), IEEE,* Retrieved on 20 November 2020, from https://ieeexplore.ieee.org/document/6565246

Althuis, Jente; Haiden Leonie (2018), Fake News: A Road Map, *NATO Strategic Communications Centre of Excellence and King's Centre for Strategic Communications, Riga,* Retrieved on 20 November 2020, from https://www.stratcomcoe.org/download/file/fid/78539

Anthony, Sebastian (2015), The first rule of zero-days is no one talks about zero days (so we'll explain), *Ars Technica (Oct. 20, 2015),* Retrieved on 20 November 2020, from https://arstechnica.com/information-technology/2015/10/the-rise-of-the-zero-day-market/

Baezner, Marie; Robin, Patrice (2017), *Hotspot Analysis: Stuxnet*, Center for Security Studies (CSS), ETH Zürich, Retrieved on 05 December 2020, from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

Barnes, Julian; Sanger, David (2020), N.S.A. Takes Step Toward Protecting World's Computers, Not Just Hacking Them, *The New York Times (Jan. 14, 2020),* Retrieved on 20 November 2020, from https://www.nytimes.com/2020/01/14/us/politics/nsa-microsoft-vulnerability.html

Becker, Gary (1968), Crime and Punishment: An Economic Approach, *Journal of Political Economy,* Vol. 76, No. 2 (Mar. - Apr. 1968), pp. 169-217, The University of Chicago Press

Bellovin, Steven; Blaze, Matt; Clark, Sandy; Landau, Susan (2014), Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, *Northwestern Journal of Technology & Intellectual Property*, Vol. *12*, Issue 1, pp. 1-63

Broad, William J.; Markoff, John; Sanger, David E. (2011), Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *N.Y. TIMES,* Jan. 15, 2011, Retrieved on 05 December 2020, from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=a

Brown, John Prather (1973), Toward an Economic Theory of Liability, The Journal of Legal Studies, Vol. 2, No. 2, pp. 323-349

Buchanan, Ben (2020), *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press

Calabresi, Guido (1961), Some Thoughts on Risk Distribution and the Law of Torts, *The Yale Law Journal*, Vol. 70, No. 4, pp. 499-553

Calabresi, Guido (1970), *The Costs of Accidents: A Legal and Economic Analysis*, New Haven: Yale University Press

Calabresi, Guido; Melamed, Douglas (1972), Property Rules, Liability Rules, and

Inalienability: One View of the Cathedral, *Harvard Law Review,* Vol. 85, No. 8, pp. 1089-1128

CEPS Task Force (2018), Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, *Centre for European Policy Studies (CEPS),* Retrieved on 20 November 2020, from https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf

Chen, Thomas (2010), Stuxnet, the real start of cyber warfare*? IEEE Network. Vol. 24, No.6, pp. 2–3,* Retrieved on 20 November 2020, from *https://doi.org/10.1109/MNET.2010.5634434*

Chen, Thomas; Abu-Nimeh, Saeed (2011), Lessons from Stuxnet, *Computer,* Vol. 44, No. 4, pp. 91–93, Retrieved on 20 November 2020, from https://doi.org/10.1109/MC.2011.115

Coase Ronald (1960), The Problem of Social Cost, *The Journal of Law & Economics,* Vol. 3, October 1960, pp. 1-44

Collins, Sean; McCombie, Stephen (2012), Stuxnet: the emergence of a new cyber weapon and its implications, *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, pp. 80-91

Cooter, Robert; Ulen, Thomas (2014), *Law and Economics (6th edition),* Pearson Education Limited

Corera, Gordon (2020), Coronavirus: Cyber-spies hunt Covid-19 research, US and UK warn, May 05, 2020, *BBC News,* Retrieved on 20 November 2020, from https://www.bbc.com/news/technology-52551023

Daniel, Michael (2014), Heartbleed: Understanding When We Disclose Cyber Vulnerabilities, *White House Blog,* 28th April 2014 ("Daniel Blog Post"), Retrieved on 30 November 2020, from https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

Dari-Mattiacci, Giuseppe; Parisi, Francesco (2005), The economics of tort law: a precis, in Backhaus, Jürgen (ed.): *The Elgar Companion to Law and Economics*, 2nd Edition, pp. 87-102, Cheltenham: Edward Elgar

De Falco, Marco (2012), Stuxnet Facts Report: A Technical and Strategic Analysis, *NATO Cooperative Cyber Defence Centre of Excellence,* Tallinn, Retrieved on 30

November 2020, from https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Delcheva, Teodora; Soesanto, Stefan (2018), Time to talk: Europe and the Vulnerability Equities Process, *European Council on Foreign Relations,* 21 March 2018, Retrieved on 30 November 2020, from https://www.ecfr.eu/article/commentary_time_to_talk_europe_and_the_vulnerability_equities_process

Egelman, Serge; Herley, Cormac (2013), Markets for zero-day exploits: ethics and implications, *NSPW '13: Proceedings of the 2013 New Security Paradigms Workshop,* pp. 41-46, Retrieved on 05 December 2020, from https://doi.org/10.1145/2535813.2535818

Elkin-Koren, Niva; Salzberger, Eli (2004), *Law, Economics and Cyberspace: The Effects of Cyberspace on the Economic Analysis of Law*, Edward Elgar Publishing Limited (UK) & Edward Elgar Publishing, Inc (USA)

Fama Eugene (1970), Efficient Capital Markets: A Review of Theory and Empirical Work, *The Journal of Finance,* Vol. 25, No. 2, pp. 383-417

Farwell, James P.; Rohozinski, Rafal (2011): Stuxnet and the Future of Cyber War, *Survival,* Vol. 53, No. 1, pp. 23-40

Faure, Michael (2016), Economic Analysis of Product Liability, in Machnikowski, Piotr (ed.), *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, Antwerp, Intersentia, pp. 619-665

Faure, Michael; Visscher, Louis; Weber, Franziska (2016), Liability for Unknown Risks - A Law and Economics Perspective, *Journal of European Tort Law*, Vol. 7, No. 2, pp. 198-228

Fidler, Mailyn (2015): Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis, *I/S: A Journal of Law and Policy for the Information Society,* Vol. 11.2, 406-483

Fischerkeller, Michael; Harknett, Richard (2018), Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace, *Lawfare blog,* 9 November 2018, Retrieved on 05 December 2020, from https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace

Frei, Stefan (2013), *The known unknowns: empirical analysis of publicly unknown*

*security vulnerabilities,* NSS Labs, Austin

Friedman, Allan; Moore, Tyler; Procaccia, Ariel (2010), Cyber-Sword v. Cyber-Shield: The Dynamics of US Cybersecurity Policy Priorities, *Center for Research on Computation & Society,* Harvard University, Retrieved on 05 December 2020, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.4819&rep=rep1&type=pdf

Ganim, Narmeen Al (2020), *Is software a product? A comparative study of EU and US law*, Master Thesis, Tilburg University, Retrieved on 05 December 2020, from http://arno.uvt.nl/show.cgi?fid=149658

Goertzel, Karen (2016), Legal liability for bad software, *CrossTalk,* Sep./Oct. 2016, Vol. 29, No. 5, pp. 23-28, Retrieved on 05 December 2020, from https://www.researchgate.net/publication/310674753

Goodin , Dan (2017), NSA-leaking Shadow Brokers just dumped its most damaging release yet, *Arstechnica*, Retrieved on 01 December 2020, from https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

Goodin, Dan (2019), Zero-day exploit prices are higher than ever, especially for iOS and messaging apps, *Ars Technica,* Jan. 7, 2019, Retrieved on 05 December 2020, from https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/

Gossart, Cédric (2014), Can Digital Technologies Threaten Democracy by Creating Information Cocoons?, In book: *Transforming Politics and Policy in the Digital Age* (Chapter 10, pp.145-154), Center for Research into Online Communities and E-Learning Systems, Belgium,

Grimes, Roger A. (2017), *Hacking the Hacker: Learn from the Experts Who Take down Hackers,* Wiley & Sons

Gross, Michael Joseph (2011), A Declaration of Cyber-War, *VANITY FAIR,* 02 March 2011, Retrieved on 05 December 2020, from https://www.vanityfair.com/news/2011/03/stuxnet-201104

Hannigan Robert (2017), How Britain's GCHQ Decides Which Secrets to Share with You, *The Cipher Brief,* Nov. 19, 2017, Retrieved on 05 December 2020, from https://www.thecipherbrief.com/column/strategic-view/britains-gchq-decides-

secrets-share

Healey, Jason (2020), Vulnerabilities, the Search for Buried Treasure, and the US Government, *OODA Network,* Retrieved on 05 December 2020, from https://www.oodaloop.com/ooda-original/2020/01/14/vulnerabilities-the-search-for-buried-treasure-and-the-us-government/

Herr, Trey (2017), Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle, *Belfer Center for Science and International Affairs (Harvard Kennedy School),* Retrieved on 05 December 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005616

Herr, Trey; Schneier, Bruce; Morris, Christopher (2017), Taking Stock: Estimating Vulnerability Rediscovery, *Belfer Center for Science and International Affairs (Harvard Kennedy School),* Retrieved on 05 December 2020, from https://www.belfercenter.org/publication/taking-stock-estimating-vulnerability-rediscovery

Herzog, Michel; Schmid, Jonas (2016): Who pays for zero-days? Balancing long-term stability in cyber space against short-term national security benefits, In book: Karsten, Friis; Ringsmose, Jens (2016): *Conflict in cyber space: theoretical, strategic and legal perspectives,* Routledge, pp.95-116

Hoffman Alex (2019), Moral Hazards in Cyber Vulnerability Markets, *The IEEE Computer Society*, Dec. 2019, Retrieved on 05 December 2020, from https://ieeexplore.ieee.org/document/8909925

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Chris (2017), The CERT Guide to Coordinated Vulnerability Disclosure, *Software Engineering Institute, Carnegie Mellon University,* Retrieved on 20 November 2020, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Howells, Geraint; Twigg-Flesner, Christian; Willett, Chris (2017), Product liability and digital products. In: Synodinou, T. E. and Jougleux, P. and Markou, C. and Prastitou, T. (eds.): *EU Internet Law*, Springer, Cham, pp. 183-195

Huang, Keman; Siegel, Michael; Stuart, Madnick (2018), Systematically Understanding the Cyber Attack Business: A Survey*, Working Paper CISL# 2018-08, July 2018,* Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology Cambridge

Hurley, John; Chen, Jim (2018), *ICCWS 2018 13th International Conference on Cyber*

*Warfare and Security*, Academic Conferences and Publishing International Limited, Mar 2018, UK

Jonathan Klick (2008): Agency Costs, Charitable Trusts, and Corporate Control: Evidence from Hershey's Kiss-off*, Columbia Law Review*, Vol. 108, No.4

Jougleux, Philippe; Synodinou, Tatiana-Eleni; Markou, Christiana; Prastitou, Thalia (Eds.) (2017), *EU Internet Law - Regulation and Enforcement*, Springer International Publishing AG

Kaplow, Louis (1992), Rules Versus Standards: An Economic Analysis, *Duke Law Journal*, Vol. 42, pp. 557-629, Retrieved on 05 December 2020, from https://scholarship.law.duke.edu/dlj/vol42/iss3/2

Kennan George (1948), *The Inauguration of Organized Political Warfare*, Redacted Version, Wilson Center Digital Archive, Retrieved on 05 December 2020, from https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c

Knapp, Eric D.; Langill, Joel Thomas (2015), Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd Edition), *Syngress Publishing,* Elsevier, Waltham

Kobayashi, Bruce (2005), Private versus social incentives in cybersecurity: Law and economics, *The Law and Economics of Cybersecurity*, Cambridge University Press 2006, pp. 13-28

Kumar, Mohit (2018), TSMC Chip Maker Blames WannaCry Malware for Production Halt, *The Hacker News*, Retrieved on 01 December 2020, from https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html

Kshetri, Nir (2017), Should spies use secret software vulnerabilities?, *The Conversation*, Retrieved on 01 December 2020, from https://theconversation.com/should-spies-use-secret-software-vulnerabilities-77770

Landes, William M.; Posner, Richard A. (1987), *The Economic Structure of Tort Law*, Cambridge, MA: Harvard University Press.

Lawson, Ewan (2019), *Conference Report: Roundtable Discussion on Disinformation in Ukraine,* Royal United Services Institute for Defence and Security Studies, UK

Lemley, Mark; McGowan, David (1998), Legal Implications of Network Economic Effects, *California Law Review,* No. 86, pp. 479 ff.

Libicki, Martin; Ablon, Lillian; Webb, Tim (2015), *The Defender's Dilemma: Charting a Course Toward Cybersecurity*, RAND Corporation, Santa Monica

Lichtman, Doug; Posner, Eric (2006), Holding Internet Service Providers Accountable, *Supreme Court Economic Review,* Vol. 14, pp. 221-259

Lindsay, Jon R. (2013), Stuxnet and the Limits of Cyber Warfare, *Security Studies*, Vol. 22, No. 3, pp. 365-404

Maurushat, Alana (2013), *Disclosure of Security Vulnerabilities: Legal and Ethical Issues,* London Heidelberg New York Dordrecht: Springer

Mayer, Jonathan (2018), Government Hacking, *The Yale Law Journal,* Vol. 127, No. 3, pp. 490-787

McConnell, Steve (2004), *Code Complete: A practical handbook of software construction*, Microsoft Press, Redmond, Washington

Nader, Ralph (1965), *Unsafe at Any Speed: The Designed-In Dangers of The American Automobile*, Grossman Publishers, New York

Nakashima, Ellen; Warrick, Joby (2012), Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *Washington Post*, Retrieved on 05 December 2020, from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Perlroth, Nicole; Sanger, David (2017), Hacks raise fear over N.S.A.'s hold on cyber-weapons, *NY Times*, 28 June 2017, Retrieved on 05 December 2020, from https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html

Philp, Catherine (2020), State-sponsored hackers 'trying to steal coronavirus vaccine secrets', *The Times,* 05 May 2020, Retrieved on 05 December 2020, from https://www.thetimes.co.uk/article/state-sponsored-hackers-trying-to-steal-coronavirus-vaccine-secrets-mrmrlzcst

Picker, Randal (2004), Cyber Security: Of Heterogeneity and Autarky, In Book: Grady, Mark F.; Parisi, Francesco (2004): *The Law and Economics of Cybersecurity,* Cambridge University Press, pp. 115-140

Pindyck, Robert; Rubinfeld, Daniel (2001), *Microeconomics (5th edition),* Prentice Hall International Inc.

Polinsky, A. Mitchell (1980), Strict liability vs. negligence in a market setting, American Economic Review, Vol. 70, pp. 363-370

Polinsky, A. Mitchell; Che, Yoen-Koo (1991), Decoupling liability: optimal incentives for care and litigation, *RAND Journal of Economics*, Vol. 22, pp. 562-570

President's Review Group (2013), *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, Retrieved on 05 December 2020, from https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world

Pupillo Lorenzo (2017), *Software Vulnerabilities Disclosure: The European Landscape*, CEPS, 31 July 2017, Brussel, Retrieved on 05 December 2020, from https://www.ceps.eu/ceps-publications/software-vulnerabilities-disclosure-european-landscape/

Radianti, Jaziar; Rich, Eliot; Gonzalez, Jose J. (2009): *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation*, 42nd Hawaii International Conference on System Sciences, IEEE, Retrieved on 05 December 2020, from https://ieeexplore.ieee.org/document/4755606

Rosenzweig, Paul (2013), *Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare*, The Great Courses, Chantilly

Sanger, David (2014), Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say, *New York Times,* 12 April 2014, Retrieved on 05 December 2020, from https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html

Schaefer, Hans-Bernd; Mueller-Langer, Frank (2008), *Strict liability versus negligence*, MPRA Paper No. 40195, Retrieved on 05 December 2020, from https://mpra.ub.uni-muenchen.de/40195/1/MPRA_paper_40195.pdf

Schneier, Bruce (2017), Who are the shadow brokers?, *The Atlantic*, May 23, 2017, Retrieved on 20 April 2020, from https://www.theatlantic.com/technology/archive/2017/ 05/shadow-brokers/527778/

Schwartz, Ari; Knake, Rob (2016), *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Retrieved on 05 December 2020, from https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf

Shavell, Steven (1980), Strict Liability versus Negligence, *The Journal of Legal Studies*, Vol. 9, No. 1, pp. 1-25

Shavell, Steven (1984), Liability for Harm versus Regulation of Safety, *The Journal of Legal Studies*, Vol. 13, No. 2, pp. 357-374

Shavell, Steven (2005), *Liability for Accidents,* Discussion Paper No. 530, Harvard Law School, Cambridge, Retrieved on 05 December 2020, from http://www.law.harvard.edu/programs/olin_center/papers/pdf/Shavell_530.pdf

Shavell, Steven (2013), A Fundamental Enforcement Cost Advantage of the Negligence Rule over Regulation, *The Journal of Legal Studies*, Vol. 42, No. 2

Shleifer, Andrei (2000), *Inefficient Markets: An introduction to behavioral finance*, Oxford University Press; 1 edition (April 20, 2000)

Shy, Oz (2008), *How to Price*, Cambridge University Press, Cambridge

Shy, Oz (2001), *The Economics of Network Industries,* Cambridge University Press, Cambridge

Shy, Oz (1995), *Industrial Organization: Theory and Applications*, The MIT Press

Skybox (2020), *2020 Vulnerability and Threats Trends*, Skybox Security Research Report, Retrieved on 05 December 2020, from https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020-VT-Trends_Executive-Summary.pdf

Swire, Peter (2004), A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?, *Journal on Telecommunications and High Technology Law*, Vol. 3, pp. 163-208

The Economist (2013): The digital arms trade, *The Economist*, Mar 30th, 2013, Retrieved on 05 December 2020, from https://www.economist.com/business/2013/03/30/the-digital-arms-trade

The Economist (2017a): Cyber-crime: Electronic bandits, *The Economist*, May 20th, 2017, pp. 67-68

The Economist (2017b): The exploits of bug hunters, *The Economist*, May 20th, 2017, Retrieved on 05 December 2020, from https://www.economist.com/science-and-technology/2017/05/18/the-exploits-of-bug-hunters

The Economist (2017c): The worm that turned, *The Economist*, May 20th, *2017,* Retrieved on 05 December 2020, from https://www.economist.com/leaders/2017/05/20/the-wannacry-attack-reveals-

the-risks-of-a-computerised-world

The Economist (2017d): Why everything is hackable?*, The Economist*, April 8th, 2017, Retrieved on 05 December 2020, from https://www.economist.com/science-and-technology/2017/04/08/computer-security-is-broken-from-top-to-bottom

The Economist (2017e): Electronic bandits, *The Economist*, May 20th-26th 2017

Trautman, Lawrence J.; Ormerod, Peter C. (2018), Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things, *University of Miami Law Review,* Vol. 72, pp. 761-826

Triaille, Jean-Paul (1990), The EEC directive of july 25, 1985 on product liability and its application to databases and information, *International Computer Law Adviser*, Vol. 5, No. 2, pp. 7-20

Varadi, Sz.; Gultekin Varkonyi, G.; Kertesz, A. (2019), Legal Issues of Social IoT Services: The Effects of Using Clouds, Fogs and AI, in Hassanien, Aboul Ella; Bhatnagar, Roheet; Khalifa, Nour Eldeen M.; Taha, Mohamed Hamed N. (2019): *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, Springer, pp. 123-138

van Erp, Judith; Faure, Michael; Nollkaemper, André; Philipsen, Niels (2019), *Smart Mixes for Transboundary Environmental Harm*, Cambridge University Press

Volz, Dustin (2020), Microsoft Releases Patch to Severe Windows Flaw Detected by NSA, *The Wall Street Journal,* Jan. 14, 2020, Retrieved on 05 December 2020, from https://www.wsj.com/articles/microsoft-releases-patch-to-severe-windows-flaw-detected-by-nsa-11579030780

Zetter, Kim (2011), How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, *WIRED*, July 11, 2011, Retrieved on 05 December 2020, from https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

## English Summary of the Thesis

Nowadays, it is not difficult to conjure up images of hacked power plants, remote-hijacked public transportation systems, etc. By exploiting hidden vulnerabilities, hackers are plundering business secrets, stealing digital consumers' records, and trying to reshape the world inconspicuously. Most of society lacks awareness of software vulnerabilities. Software vendors seem unlikely to discuss flaws in their products publicly, and the related markets of vulnerabilities are often opaque. This thesis tries to introduce its readers to a structured discussion and analysis of software vulnerabilities vis-à-vis the challenges of cyberattacks.

This thesis focuses on an analysis of software vulnerabilities and their relevance to cybersecurity from an economic perspective, and it discusses the role of law and regulation designed to address problems of vulnerabilities and cybersecurity utilizing the law and economics approach.

A software vulnerability has its intrinsic value and a life cycle. There are people who search for these vulnerabilities - the bug hunters, and there are three markets for vulnerabilities - white, grey, and black. The assumption of profit maximization in traditional economics also applies to bug hunters. Moreover, this thesis finds that the nature of the white market vis-à-vis the grey or black market is much more competitive. Among the factors that influence the price level of a software vulnerability in the black market, the bounty price (white market price) is particularly worthy of attention.

This thesis finds that the practice of governments to retain vulnerabilities is acceptable in the short run for the purpose of legal enforcement or intelligence, given the advanced encryption and anonymization technologies used by criminals. However, in the long run, government agencies should avoid vulnerability transactions. Furthermore, government agencies should give the utmost attention to how to protect their vulnerability stockpiles from being stolen.

The empirical results of this thesis prove that a market failure exists at least to some

extent in relation to vulnerabilities. There was no significant market pressure upon the software vendor even when the software had been proved seriously risky by a severe cyberattack. Possible avenues to correct this market failure could be found in private law, administrative law, or other means of central intervention. This thesis advocates a solution of jointly using liability rules and safety regulation backed by a public fine (regulation backed by an administrative fine) for the harm caused by a vulnerability. More details are provided by means of an economic model. It is a combination of torts and regulation (ex-ante and ex-post), which is in line with the suggestions made in Shavell (1984), and Faure, Visscher & Weber (2016).

**Samenvatting van de thesis**

Vandaag de dag is het niet moeilijk om beelden op te roepen van gehackte energiecentrales, op afstand gekaapte publieke transportsystemen, etc. Door gebruik te maken van verborgen kwetsbaarheden, plunderen hackers bedrijfsgeheimen, stelen zij digitale consumentengegevens en proberen zij onopvallend de wereld om te vormen. De meeste mensen zijn zich niet bewust van de softwarekwetsbaarheden. Softwareverkopers zullen de onvolkomenheden in hun producten waarschijnlijk niet publiekelijk bespreken en de verwante markten van kwetsbaarheden zijn vaak ondoorgrondelijk. Deze thesis wil haar lezers laten kennismaken met een gestructureerde discussie en analyse van softwarekwetsbaarheden in relatie tot de uitdagingen van cyberaanvallen.

Deze thesis focust op een analyse van softwarekwetsbaarheden en hun relevantie voor cybersecurity vanuit een economisch perspectief en bespreekt de rol van wet- en regelgeving, ontworpen om de problemen van kwetsbaarheden en cybersecurity aan te pakken met behulp van een rechtseconomische benadering.

Een softwarekwetsbaarheid heeft zijn eigen intrinsieke waarde en levenscyclus. Er zijn mensen die op zoek gaan naar deze kwetsbaarheden, de zgn. ‘bug hunters’, en er zijn drie markten voor kwetsbaarheden: wit, grijs en zwart. De aanname van winstmaximalisatie in de traditionele economie is ook van toepassing op de bug hunters. Bovendien maakt deze thesis duidelijk dat er veel meer concurrentie is in de witte dan in de grijze en zwarte markt. Van de factoren die het prijsniveau van een softwarekwetsbaarheid op de zwarte markt beïnvloeden, is vooral de premieprijs (witte marktprijs) van bijzonder belang.

Deze thesis oordeelt dat de praktijk van overheden om kwetsbaarheden te handhaven acceptabel is op korte termijn ten behoeve van de rechtshandhaving of inlichtingendiensten, gelet op de door criminelen gebruikte geavanceerde versleutelings- en anonimiseringstechnologieën. Op lange termijn moeten overheidsinstanties echter kwetsbaarheidstransacties vermijden. Bovendien moeten

overheidsinstanties de grootste aandacht besteden aan hoe zij hun kwetsbaarheidsvoorraden tegen diefstal kunnen beschermen.

De empirische resultaten van deze thesis tonen aan dat er ten minste in bepaalde mate sprake is van een marktfalen in relatie tot kwetsbaarheden. Er was geen significante marktdruk op de softwareverkoper, zelfs niet als de software een aantoonbaar serieus risico liep op een ernstige cyberaanval. Mogelijke middelen om dit marktfalen te corrigeren zijn te vinden in het privaatrecht, administratief recht of andere middelen van centrale interventie. Deze thesis bepleit een oplossing voor het gezamenlijk gebruiken van aansprakelijkheidsregels en veiligheidsregulering ondersteund door een publiekrechtelijke boete (regulering ondersteund door een administratieve boete) voor de schade veroorzaakt door de kwetsbaarheid. Meer details worden gegeven door middel van een economisch model. Het is een combinatie van aansprakelijkheidsregels en regulering (ex ante en ex post), die in lijn ligt met de suggesties gedaan in Shavell (1984), en Faure, Visscher & Weber (2016).