NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

THIAGO ARAUJO MONTEIRO

BSc in Computer Science and Engineering

CREATING A THREAT MODELING PROTOCOL FOR NON-HIERARCHICAL ORGANIZATIONS

Dissertation Plan

MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon

Draft: *December 19, 2024*

NOVA SCHOOL OF
SCIENCE & TECHNOLOGY

DEPARTMENT OF
COMPUTER SCIENCE

CREATING A THREAT MODELING PROTOCOL FOR NON-HIERARCHICAL ORGANIZATIONS

THIAGO ARAUJO MONTEIRO

BSc in Computer Science and Engineering

Adviser: Kevin Gallagher
Full Professor, NOVA University Lisbon

Dissertation Plan
MASTER IN COMPUTER SCIENCE AND ENGINEERING

NOVA University Lisbon
Draft: *December 19, 2024*

Abstract

Regardless of the language in which the dissertation is written, usually there are at least two abstracts: one abstract in the same language as the main text, and another abstract in some other language.

Keywords: One keyword, Another keyword, Yet another keyword, One keyword more, The last keyword

Resumo

Independentemente da língua em que a dissertação está escrita, geralmente esta contém pelo menos dois resumos: um resumo na mesma língua do texto principal e outro resumo numa outra língua.

Palavras-chave: Primeira palavra-chave, Outra palavra-chave, Mais uma palavra-chave, A última palavra-chave

Contents

List of Figures

Acronyms

CGTP Confederação Geral dos Trabalhadores Portugueses *(p. 7)*

DAO Decentralized Autonomous Organization *(p. 6)*

PCP Partido Comunista Português *(p. 7)*

STRIDE Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege *(p. 5)*

1

Introduction

"The very soldiers who had no courage in the White army yesterday are very brave in the Red Army today; such is the effect of democracy."

Mao Tsé-Tung

1.1 Governança Organizacional: Uma Perspectiva Histórica

A governança organizacional reflete as estruturas sociais, econômicas e tecnológicas vigentes em cada época. Desde os primeiros agrupamentos humanos até as organizações complexas da contemporaneidade, as formas de organizar o poder e a tomada de decisão foram moldadas para responder a contextos específicos. O modelo hierárquico, adotado amplamente, emergiu como solução para demandas de controle e eficiência, mas a história também registra experimentos que desafiaram essa lógica.

Mesmo em sistemas participativos históricos, como a democracia ateniense, a horizontalidade enfrentou limitações de inclusão e praticidade [2]. Durante a Revolução Industrial, a centralização hierárquica intensificou-se para lidar com o crescimento e a complexidade organizacional. Por outro lado, cooperativas e movimentos sindicalistas do século XIX começaram a esboçar alternativas à centralização absoluta, apontando novos caminhos para a governança [8, 21].

No século XX, os avanços tecnológicos e as novas teorias organizacionais puseram em xeque a inevitabilidade das hierarquias rígidas. Nesse contexto, cooperativas modernas e redes descentralizadas demonstraram a possibilidade de alinhar eficiência a valores igualitários [26]. Ao mesmo tempo, tecnologias de vigilância em massa tendem a reforçar estruturas centralizadoras, enquanto ferramentas como o blockchain catalisam processos de descentralização, ampliando o alcance de modelos horizontais [25]. Essa evolução histórica lança as bases para entender, a seguir, os desafios contemporâneos de segurança em estruturas não-hierárquicas.

1.2 A Segurança Horizontal em Tempos de Interconexão

No mundo interconectado atual, organizações horizontais enfrentam desafios de segurança específicos. A ausência de hierarquia formal dificulta ataques centralizados, mas exige uma redefinição da gestão da confiança. Em sistemas de confiança distribuída, como os utilizados em organizações descentralizadas baseadas em blockchain, a segurança depende de mecanismos que substituem líderes formais por processos participativos e algoritmos orientados à transparência e ao consenso [17].

Modelos tradicionais de segurança, como STRIDE e árvores de ataque, fornecem bases sólidas para análise de ameaças, mas nem sempre se adaptam à complexidade das estruturas descentralizadas [7]. Por outro lado, tecnologias como a criptografia colaborativa [4, 1] permitem que múltiplos membros contribuam para a proteção de dados sem comprometer a horizontalidade.

Essas abordagens já demonstram um avanço significativo: a segurança pode ser concebida de forma coerente com princípios democráticos, preservando a horizontalidade. Compreender tais desafios é o primeiro passo para a proposição de um protocolo de segurança específico, que será discutido no próximo capítulo.

1.3 Protocolo de Segurança para Organizações Não-Hierárquicas

Esta pesquisa propõe um protocolo de segurança que não apenas preserva a horizontalidade, mas a converte em um diferencial estratégico. Ao invés de considerar a ausência de hierarquia como vulnerabilidade, buscou-se demonstrar que ela pode fornecer resiliência diante de cenários adversos. Tal esforço preenche uma lacuna na literatura sobre segurança em estruturas horizontalizadas, oferecendo diretrizes práticas para organizações comprometidas com a governança democrática.

O protocolo fundamenta-se em valores participativos, na análise de casos reais de cooperativas e redes comunitárias, e em abordagens metodológicas orientadas à eficiência e à transparência. Por exemplo, imagine uma cooperativa de trabalhadores que gerencia recursos digitais sensíveis: como assegurar a proteção contra fraudes internas e ataques externos sem recorrer a estruturas autoritárias? O protocolo aqui delineado oferece mecanismos de consenso, transparência, criptografia colaborativa e modelagem de ameaças adaptada, respondendo a esse tipo de questionamento.

Assim, ao alinhar eficiência técnica, participação coletiva e acesso igualitário à informação, o protocolo se diferencia de abordagens tradicionais. Antes de detalhar seus elementos, é necessário delimitar o escopo da pesquisa para garantir precisão analítica.

1.4 Delimitando o Escopo da Pesquisa

A variedade de arranjos organizacionais horizontais é ampla. Para uma análise mais profunda, esta pesquisa concentra-se em estruturas plenamente horizontais que operam

sob princípios de confiança distribuída e governança democrática, como cooperativas de trabalhadores e redes comunitárias [8, 21]. Ao excluir organizações híbridas, busca-se compreender o cerne da relação entre horizontalidade e segurança, esclarecendo a eficácia do protocolo proposto em cenários puros. Futuras investigações poderão, então, integrar elementos híbridos, ampliando a aplicabilidade do conhecimento gerado.

1.5 Contribuições Esperadas

Esta pesquisa espera avançar a compreensão teórica da segurança em estruturas horizontais, abordando lacunas evidenciadas por [13] e [23], que ressaltam a necessidade de ferramentas específicas para tais contextos. No plano prático, espera-se oferecer um conjunto de recomendações que combine eficiência, participação coletiva e transparência na proteção de dados e processos.

Ao ampliar o repertório de soluções, a segurança não se torna um obstáculo, mas uma oportunidade de aprofundar a democratização organizacional. Assim, o protocolo contribui para o desenvolvimento de organizações em que a horizontalidade não é meramente um ideal normativo, mas uma estratégia efetiva contra ameaças complexas.

1.6 Estrutura da Tese

Após esta introdução, o capítulo de fundamentação teórica definirá conceitos centrais, como modelagem de ameaças, governança horizontal e confiança distribuída. Em seguida, o capítulo de trabalhos relacionados analisará estudos pré-existentes, como [4, 1], situando o protocolo proposto no debate acadêmico. O capítulo de design detalhará o protocolo, seus componentes e os métodos de avaliação. Por fim, as conclusões sintetizarão os achados e sugerirão direções para pesquisas futuras, reforçando o papel da horizontalidade como aliada da segurança em um mundo cada vez mais interconectado.

2

Background

2.1 Fundamentos da Modelagem de Ameaças

A modelagem de ameaças é um componente central da cibersegurança, pois permite identificar ativos valiosos, analisar potenciais vetores de ataque e estabelecer controles capazes de mitigar riscos. Esse processo não se restringe a fatores técnicos: ele integra também elementos organizacionais e humanos, tornando a avaliação de segurança mais ampla e coerente com a realidade das organizações. A relevância desse tema torna-se evidente no cenário atual, marcado pela rápida evolução tecnológica e pela diversificação constante das ameaças.

Estudos como [13], [14] e [23] demonstram que uma abordagem estruturada e flexível é essencial para acompanhar ambientes em constante mudança. Ao adotar a perspectiva do adversário, conforme sugerido em [12], antecipam-se cenários complexos, fortalecendo a resiliência dos sistemas e proporcionando uma visão mais realista das vulnerabilidades a serem tratadas. Esse ponto é especialmente relevante em organizações que buscam maior autonomia decisória e flexibilidade estrutural.

Adicionalmente, a experiência da Microsoft, documentada em [19], destaca a importância de envolver uma ampla gama de stakeholders e a utilização de ferramentas colaborativas para identificar riscos emergentes. Esses elementos são cruciais para endereçar não apenas vulnerabilidades técnicas, mas também questões organizacionais e humanas que impactam a segurança.

2.1.1 Definições Conceituais

A modelagem de ameaças pode ser entendida como um esforço sistemático de proteção, no qual se mapeiam pontos fracos e se antecipam possíveis ataques a partir da análise do comportamento adversário. Dessa forma, além do contexto puramente técnico, aspectos organizacionais e humanos são contemplados, conferindo uma perspectiva holística que auxilia na identificação e mitigação de riscos emergentes. Trabalhos como [13] e [14] reforçam a importância desse olhar abrangente, enquanto [23] destaca a necessidade de metodologias flexíveis, capazes de acompanhar a evolução tecnológica.

2.1.2 Principais Metodologias

Entre as metodologias amplamente discutidas estão o Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), as árvores de ataque e os frameworks baseados em cenários [20]. A participação ativa de stakeholders no processo de modelagem, sugerida em [22], mostra-se especialmente importante em ambientes menos hierarquizados, incentivando maior engajamento e responsabilidade coletiva.

A documentação [18] fornece uma visão geral dos métodos existentes, destacando a necessidade de adaptação das ferramentas de acordo com o contexto da organização. Em particular, os frameworks baseados em cenários permitem identificar padrões de ataque menos óbvios, incluindo ameaças internas combinadas com ataques externos.

Para ilustrar seu uso, considere duas situações práticas. Na primeira, uma startup de tecnologia baseada em microserviços emprega o STRIDE para identificar vetores de ataque, descobrindo que elevação de privilégios e negação de serviço são riscos-chave. Como resposta, implementam-se controles de acesso mais robustos e mecanismos de limitação de tráfego.

Na segunda, uma empresa do setor financeiro recorre às árvores de ataque para analisar ações potenciais de um invasor interessado em comprometer sistemas de autenticação de múltiplos fatores. Ao decompor objetivos e passos necessários ao ataque, a organização consegue estabelecer barreiras específicas em cada etapa, aumentando assim a segurança do sistema.

Da mesma forma, frameworks baseados em cenários permitem simular situações complexas, como ataques internos e externos simultâneos, fornecendo insights sobre a resiliência e a prontidão da empresa diante de eventos adversos.

A integração de diferentes metodologias e o uso de criptografia colaborativa [1] ou abordagens híbridas [24] potencializam a eficácia da modelagem de ameaças. Para facilitar a consulta, uma tabela resumo poderia ser incluída, comparando o STRIDE, as árvores de ataque e os frameworks de cenários em relação a escopo, complexidade e tipos de ameaças endereçadas.

2.2 Taxonomia de Estruturas Organizacionais

Compreender como diferentes estruturas organizacionais influenciam as práticas de segurança é essencial para adaptar estratégias de modelagem de ameaças a contextos específicos. Nesta seção, analisamos tipologias de organizações e suas implicações para a mitigação de riscos. Ao entender as peculiaridades de estruturas hierárquicas, horizontais ou sem liderança, é possível direcionar abordagens de segurança mais ajustadas ao perfil da organização (ver [8] e [11]).

2.2.1 Estruturas Tradicionais Hierárquicas

Organizações com estruturas hierárquicas bem definidas contam com linhas claras de autoridade e comunicação. Essa abordagem facilita a delegação e o controle, mas pode, ao mesmo tempo, concentrar vulnerabilidades. Por exemplo, o comprometimento de um ponto de decisão-chave pode ter impacto desproporcional sobre todo o sistema. Estudos como [27] e [25] mostram que hierarquias rígidas podem reforçar desigualdades de poder e expor áreas críticas a ameaças internas.

2.2.2 Organizações Horizontais

Organizações horizontais, caracterizadas pela autonomia individual e pela ausência de hierarquias rígidas [17, 5], favorecem a inovação e a flexibilidade. Entretanto, a coordenação de recursos e a tomada de decisão coletiva representam desafios. Nesse contexto, tecnologias descentralizadas, como o blockchain, podem fornecer mecanismos de verificação independentes, aumentando a segurança e a transparência.

Considere uma cooperativa de produtores de software open-source. Nesse ambiente, cada membro contribui com código e revisões, e a segurança é garantida por uma verificação contínua da comunidade. A ausência de um líder formal não significa falta de governança: regras de contribuição e protocolos de segurança são acordados coletivamente, e a confiança é reforçada por auditorias públicas do código e sistemas de reputação. Esses arranjos assemelham-se em muitos aspectos a uma Decentralized Autonomous Organization (DAO), pois dependem de mecanismos descentralizados para coordenação e controle. Estudos [1] sugerem que criptografia colaborativa e abordagens participativas fortalecem a resiliência em tais contextos, reduzindo a dependência de pontos únicos de falha.

Além disso, a experiência de iniciativas educacionais, como as analisadas em [15], indica que estruturas horizontais podem fomentar maior engajamento e autonomia individual, contribuindo também para a sustentabilidade das próprias dinâmicas organizacionais.

2.2.3 Modelos Organizacionais Sem Liderança

Em modelos sem liderança formal, a governança distribuída apoia-se em algoritmos de reputação, sistemas colaborativos e processos decisórios transparentes. Conforme analisado em [10, 21], esses arranjos podem mitigar ameaças complexas ao distribuir responsabilidades de modo equilibrado. Ao invés de depender de uma figura central, a segurança emerge do próprio tecido organizacional, que integra continuamente a perspectiva adversária em sua dinâmica interna, aumentando a resiliência de forma natural e adaptativa.

Experiências relatadas em [6] mostram que modelos sem liderança podem implementar práticas inovadoras de segurança, como redes descentralizadas de resposta a ameaças,

que se ajustam dinamicamente às necessidades do ambiente, promovendo robustez frente a ataques inesperados.

2.3 Centralismo Democrático

Ao analisar as diferentes estruturas organizacionais e suas implicações para a segurança, é útil considerar teorias que equilibram participação interna e eficiência operacional. O centralismo democrático, abordado em [16], [3] e [28], propõe um modelo de governança que busca harmonizar a tomada de decisão coletiva com mecanismos de coordenação bem definidos.

2.3.1 Origens Teóricas

A teoria do centralismo democrático, descrita em [21], procura alinhar a eficiência da centralização com a legitimidade da participação. Nesse sentido, o processo decisório inclui o debate interno e a participação ativa dos membros, seguido pela implementação disciplinada das decisões, visando ao bem-estar coletivo. Por exemplo, o Partido Comunista Português (PCP) adota essa abordagem, como indicado em [16].

2.3.2 Aplicações Contemporâneas

Em contextos contemporâneos, o centralismo democrático pode ser adaptado a formatos digitais e distribuídos. Por exemplo, [9] explora a coordenação de equipes dispersas por meio de ferramentas on-line, enquanto [4] sugere o uso de tecnologias emergentes para reforçar a disciplina interna sem inibir a inovação. Dessa maneira, o modelo preserva sua capacidade de resposta, mesmo quando aplicado a redes complexas. Em âmbito sindical, a Confederação Geral dos Trabalhadores Portugueses (CGTP) também oferece um exemplo de como princípios similares podem estruturar a tomada de decisão coletiva [3].

2.3.3 Implicações para Governança

As implicações do centralismo democrático para a segurança incluem a necessidade de processos decisórios transparentes, confiança distribuída e mecanismos reputacionais para aferir a confiabilidade dos participantes [17]. Tecnologias mencionadas em [1] podem fornecer ferramentas criptográficas que reforçam a segurança, garantindo a resiliência dos sistemas em face de ameaças externas e internas.

Considerações Finais

Ao longo deste capítulo, foram apresentados conceitos, metodologias e estruturas organizacionais que se relacionam com a modelagem de ameaças. Vimos que não existe uma

abordagem única capaz de atender a todos os contextos: a escolha das metodologias e ferramentas depende das características específicas da organização, da natureza das ameaças enfrentadas e do grau de centralização ou descentralização do poder decisório. Modelos híbridos, que combinam flexibilidade técnica com participação distribuída, emergem como alternativas promissoras, especialmente em ambientes onde a colaboração e a resiliência são ativos estratégicos. Dessa forma, as organizações podem adaptar suas estratégias de segurança de maneira eficiente e alinhada às demandas contemporâneas.

3

Related Work

3.1 ABC

4

Design

4.1 Horizontality as an Asset

We also show some stuff which is not that common!

5 Conclusion

5.1 rest

We also show some stuff which is not that common!

Bibliography

[1] G. Almashaqbeh, A. Bishop, and J. Cappos. "ABC: A Cryptocurrency-Focused Threat Modeling Framework". In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2019, pp. 859–864. DOI: 10.1109/INFCOMW.2019.8845101 (cit. on pp. 2, 3, 5–7).

[2] C. W. Blackwell. "Athenian Democracy: An Overview". In: *Dēmos: Classical Athenian Democracy*. Ed. by C. W. Blackwell. © 2003, C.W. Blackwell. www.stoa.org: The Stoa: A Consortium for Electronic Publication in the Humanities, 2003. URL: http://www.stoa.org (cit. on p. 1).

[3] *Estatutos da Confederação Geral dos Trabalhadores Portugueses – Intersindical Nacional: Declaração de Princípios e Objectivos Programáticos*. Acesso em: 08 dez. 2024. Confederação Geral dos Trabalhadores Portugueses (CGTP), 2020. URL: https://www.cgtp.pt/images/images/2020/02/ESTATUTOSCGTP.pdf (cit. on p. 7).

[4] K. Gallagher et al. "COLBAC: Shifting Cybersecurity from Hierarchical to Horizontal Designs". In: *Proceedings of the 2021 New Security Paradigms Workshop*. NSPW '21. Virtual Event, USA: Association for Computing Machinery, 2022, pp. 13–27. ISBN: 9781450385732. DOI: 10.1145/3498891.3498903. URL: https://doi.org/10.1145/3498891.3498903 (cit. on pp. 2, 3, 7).

[5] P. Gerbaudo. "Social media teams as digital vanguards: The question of leadership in the management of key Facebook and Twitter accounts of Occupy Wall Street, Indignados and UK Uncut". In: *Information, Communication & Society* 20.2 (2017), pp. 185–202. DOI: 10.1080/1369118X.2016.1161817. URL: https://doi.org/10.1080/1369118X.2016.1161817 (cit. on p. 6).

[6] P. Herbst. "Non-Hierarchical Forms of Organization". In: *Acta Sociologica* 19.1 (1976), pp. 65–75. DOI: 10.1177/000169937601900106. URL: https://doi.org/10.1177/000169937601900106 (cit. on p. 6).

[7] S. Hussain et al. "Threat Modelling Methodologies: A Survey". In: vol. 26. 2014-01, pp. 1607–1609. URL: https://api.semanticscholar.org/CorpusID:111533730 (cit. on p. 2).

[8] R. Jackall and H. M. Levin, eds. *Worker Cooperatives in America*. Berkeley and Los Angeles, California: University of California Press, 1984. ISBN: 0-520-05117-3 (cit. on pp. 1, 3, 5).

[9] A. Kavada. "Creating the collective: social media, the Occupy Movement and its constitution as a collective actor". In: *Information, Communication & Society* 18.8 (2015), pp. 872–886. DOI: 10.1080/1369118X.2015.1043318. eprint: https://doi.org/10.1080/1369118X.2015.1043318. URL: https://doi.org/10.1080/1369118X.2015.1043318 (cit. on p. 7).

[10] A. Kavada and T. Poell. "From Counterpublics to Contentious Publicness: Tracing the Temporal, Spatial, and Material Articulations of Popular Protest Through Social Media". In: *Communication Theory* 31.2 (2020-10), pp. 190–208. ISSN: 1050-3293. DOI: 10.1093/ct/qtaa025. eprint: https://academic.oup.com/ct/article-pdf/31/2/190/37900340/qtaa025.pdf. URL: https://doi.org/10.1093/ct/qtaa025 (cit. on p. 6).

[11] J. W. Kuyper and J. S. Dryzek. "Real, not nominal, global democracy: A reply to Robert Keohane". In: *International Journal of Constitutional Law* 14.4 (2017-01), pp. 930–937. ISSN: 1474-2640. DOI: 10.1093/icon/mow063. eprint: https://academic.oup.com/icon/article-pdf/14/4/930/9607155/mow063.pdf. URL: https://doi.org/10.1093/icon/mow063 (cit. on p. 5).

[12] N. R. Mead et al. "A hybrid threat modeling method". In: *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002* (2018) (cit. on p. 4).

[13] S. Myagmar, A. J. Lee, and W. Yurcik. "Threat modeling as a basis for security requirements". In: (2005) (cit. on pp. 3, 4).

[14] P. Nancy R. Mead. *Advanced Threat Modeling (ATM)*. Tech. rep. This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. Pittsburgh, PA 15213: Carnegie Mellon University, 2017. URL: permission@sei.cmu.edu (cit. on p. 4).

[15] J. Pacheco. *Escola da Ponte: Formação e Transformação da Educação*. Editora Vozes, 2008. ISBN: 9788532636461 (cit. on p. 6).

[16] P. C. Português. *Programa e Estatutos do PCP*. Revisão tipográfica: Edições «Avante!». Impressão: Papelmunde — SMG, Lda. Lisboa, Portugal, 2013. URL: https://www.pcp.pt/estatutos-do-pcp (cit. on p. 7).

[17] Y. Saito and J. A. Rose. "Reputation-based Decentralized Autonomous Organization for the Non-Profit Sector: Leveraging Blockchain to Enhance Good Governance". In: *Frontiers in Blockchain* 5 (2023). ISSN: 2624-7852. DOI: 10.3389/fbloc.2022.1083647. URL: https://www.frontiersin.org/articles/10.3389/fbloc.2022.1083647 (cit. on pp. 2, 6, 7).

[18] N. Shevchenko et al. "Threat modeling: a summary of available methods". In: *Software Engineering Institute | Carnegie Mellon University* (2018), pp. 1–24 (cit. on p. 5).

[19] A. Shostack. "Experiences Threat Modeling at Microsoft". In: *MODSEC@ MoDELS* (2008) (cit. on p. 4).

[20] F. Shull et al. *Evaluation of Threat Modeling Methodologies*. Tech. rep. Approved for public release and unlimited distribution. SEI Research Review 2016. DM-0004095. Carnegie Mellon University, Software Engineering Institute, 2016-10. URL: https://insights.sei.cmu.edu/documents/4027/2016_017_001_474200.pdf (cit. on p. 5).

[21] M. A. Sitrin. *Everyday Revolutions: Horizontalism and Autonomy in Argentina*. London, UK; New York, USA: Zed Books Ltd, 2012. ISBN: 9781780320502 (cit. on pp. 1, 3, 6, 7).

[22] J. Slupska et al. "Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity". In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI EA '21. Yokohama, Japan: Association for Computing Machinery, 2021. ISBN: 9781450380959. DOI: 10.1145/3411763.3451731. URL: https://doi.org/10.1145/3411763.3451731 (cit. on p. 5).

[23] P. Torr. "Demystifying the threat modeling process". In: 3.5 (2005), pp. 66–70. DOI: 10.1109/MSP.2005.119 (cit. on pp. 3, 4).

[24] J. Von Der Assen et al. "CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling". In: *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2022, pp. 189–196. DOI: 10.1109/CSR54599.2022.9850283 (cit. on p. 5).

[25] L. Winner. "Do Artifacts Have Politics?" In: *Daedalus* 109.1 (1980), pp. 121–136. ISSN: 00115266. URL: http://www.jstor.org/stable/20024652 (visited on 2024-12-08) (cit. on pp. 1, 6).

[26] C. Wright. *Worker Cooperatives and Revolution: History and Possibilities in the United States*. First Edition. Copyright © 2014 Chris Wright. All rights reserved. No part of this publication may be reproduced without prior written permission. Bradenton, Florida, USA: BookLocker.com, Inc., 2014. ISBN: 978-1-63263-432-0 (cit. on p. 1).

[27] W. Xiong and R. Lagerström. "Threat modeling - A systematic literature review". In: 84 (2019), pp. 53–69. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.03.010. URL: https://www.sciencedirect.com/science/article/pii/S0167404818307478 (cit. on p. 6).

[28] G. Yang. "Still a Century of the Chinese Model? Exploring Dimensions of Democratic Centralism". In: *Chinese Political Science Review* 1.1 (2016), pp. 171–189. DOI: 10.1007/s41111-016-0005-3. URL: https://doi.org/10.1007/s41111-016-0005-3 (cit. on p. 7).