 doi:10.20944/preprints202003.0217.v1

Artificial intelligence, machine learning and real-time probabilistic data for cyber risk (super) - forecasting

Red teaming the connected world

Petar Radanliev
UNIVERSITY OF OXFORD Department of Engineering Science

 doi:10.20944/preprints202003.0217.v1

University of Oxford
Department of Engineering Science
Pre-print - prior to peer-review

***Corresponding author details**: Petar Radanliev, Post-Doctoral Research Associate, University of Oxford, Engineering Sciences Department, Oxford e-Research Centre, 7 Keble Road, Oxford, England, OX1 3QG, petar.radanliev@oerc.ox.ac.uk [1]*

Authors: Petar Radanliev[1], David De Roure[1]; Kevin Page[1]; Max Van Kleek[2]; Rafael Mantilla Montalvo[3]; Omar Santos[3]; La'Treall Maddox[3]; Stacy Cannady[3]; Pete Burnap[4], Eirini Anthi[4], Carsten Maple[5]

Author affiliations and co-author email addresses: [1]Oxford e-Research Centre, 7 Keble Road, Oxford, OX1 3QG, Department of Engineering Sciences, University of Oxford, UK; [2]Department of Computer Science, University of Oxford, UK; [3]Cisco Research Centre, Research Triangle Park, USA; [4]School of Computer Science and Informatics, Cardiff University; MG Cyber Security Centre, University of Warwick

Funding: This work was funded by the UK EPSRC [with the PETRAS projects: RETCON and CRatE, grant number: EP/S035362/1, EP/N023013/1, EP/N02334X/1] and by the Cisco Research Centre [grant number 1525381].

Acknowledgments: Eternal gratitude to the Fulbright Scholar Project.

 doi:10.20944/preprints202003.0217.v1

University of Oxford
Department of Engineering Science
Pre-print - prior to peer-review

Abstract

This paper surveys deep learning algorithms, IoT cyber security and risk models, and established mathematical formulas to identify the best approach for developing a dynamic and self-adapting system for predictive cyber risk analytics supported with Artificial Intelligence and Machine Learning and real-time intelligence in edge computing. The paper presents a new mathematical approach for integrating concepts for cognition engine design, edge computing and Artificial Intelligence and Machine Learning to automate anomaly detection. This engine instigates a step change by applying Artificial Intelligence and Machine Learning embedded at the edge of IoT networks, to deliver safe and functional real-time intelligence for predictive cyber risk analytics. This will enhance capacities for risk analytics and assists in the creation of a comprehensive and systematic understanding of the opportunities and threats that arise when edge computing nodes are deployed, and when Artificial Intelligence and Machine Learning technologies are migrated to the periphery of the internet and into local IoT networks.

Introduction

Recent studies on Artificial Intelligence and Machine Learning (AI/ML) perspectives on mobile edge computing [1] lack detail, but provide guidance on how data can be processed [2]–[9] in real-time, reducing edge-cloud delay [10] and inform on the topic of cognitive cyber security at the edge. This paper is focused on the topic of predicting cyber risk loss magnitude through dynamic analytics of cyber-attack threat event frequencies. Challenges that need to be addressed are mainly socio-technical, relating strongly to technology, regulation, economics, interventions, and directly relates to industries and their supply chains and control systems. For example, investigating the perceptions of risk and trustworthiness that emerge as a result of machine agency, which interact with regulation, standards and policy on the one hand and design and engineering on the other, spanning the physical and behavioural sciences. But the specific focus of this paper is on integrating AI/ML in the data collection and analytics of risk through fog computing (i.e. use of edge devices) for forward-facing predictive outputs. We investigate a scenario where an organisation has implemented all the security recommendations (e.g. NIST), but the risk remains from uncertain and unpredictive attack vectors at the edge of the network.

A red teaming approach is then applied to identify IoT systems that are mostly affected by a few types of network risk event. Those include: Eavesdropping Attacks, Denial of Service (DoS) and Distributed DoS (DDoS), Spoofing Attacks, and Man-in-the-Middle attacks (MITM). To describe briefly the relationship between these types of attacks, Eavesdropping Attacks is used for listening IoT communications without the transmission appearing abnormal, hence making it difficult to detect. After Eavesdropping Attacks has gained authorisation access, Spoofing Attacks are used to send spoofed traffic with a legitimate access to IoT network. The MITM is just an advanced Spoofing Attack where adversary is positioned between two IoT devices and independently intercepts data and communicates between endpoints, collecting sensitive information, dropping packets, and causing different security vulnerabilities. The DoS and DDoS floods the IoT devices network with traffic, this overloads the communication and exhausts the network, leading to IoT devices being unable to communicate. As simple as it is, this is the most common and most dangerous IoT attack. The small computation capability at the edge devices, make DDoS attacks really difficult to resolve. While new cyber security is constantly been developed (e.g. ISO 3000), the level of cyber-attack sophistication is also increasing [11] (e.g. the Mirai variants ‘VPN filter’ is delivered in multiple stages with modularised payload; ‘TORii’ uses its own encryption and evasion tactic). Considering these continuous changes, to assess the effectiveness of cybersecurity, we need cyber analytic approaches that can handle real time intelligence in the form of probabilistic data collected at the edge. But the effectiveness of cybersecurity should not only be measured by the

protection of cyberspace, but also with the protection of assets that can be reached via cyberspace [12].

Research methodology

Quantitative risk impact estimation is needed for estimating cyber security and cyber risk [13], [14] at the edge [15]. Our argument is that without a dynamic real-time probabilistic risk data and cyber risk analytics enhanced with AI/ML, these estimations can be outdated and imprecise. Additionally, the use of red-teaming is a way of explicitly addressing attack as well as defence. We are concerned not just with securing a system, but to acknowledge that failure and compromise will occur and address how the system responds in these circumstances. This is an important methodological principle which distinguishes out work within the cybersecurity domain. Recent literature confirms diverse cyber risks from IoT systems [16], including risks in IoT ecosystems [17] and IoT environments [18], such as risk from smart homes [19], [20], the Industrial IoT [21], and challenges in security metrics [22]. Cybersecurity solutions for specific IoT risks are also emerging at a fast rate, such as new models on opportunities and motivations for reducing cyber risk [23], adaptive intrusion detection [24], security economic by design [25], highlighting the privacy requirements [26] and strategies for achieving privacy [27]. But the usage of traditional risk assessments in new IoT technologies is strongly criticised [28]–[30]. Therefore, our methodology is based on mathematical principles and quantitative data. In recent publications on this topic [31]–[33], we discovered that the lack of probabilistic data leads to qualitative cyber risk assessment approaches, where the outcome represents a speculative assumption. Emerging quantitative models are effectively designed with ranges and confidence intervals based on expert opinions and not probabilistic data [34].

Survey of AI/ML algorithms

The AI/ML are essential for advancing beyond the limitations of Value-at-Risk (VaR) models [35], where Bayesian and frequentist methods are applied with and beyond VaR models [36]. This requires federated learning and blockchain based decentralised AI architecture where AI processing shifts from the cloud to the edge and the AI workflow is moved and data restricted to the device [37]. Current gaps in cyber risk analytics are in the areas of descriptive, predictive, and prescriptive analytics [38]. Hence, a survey of AI/ML applications is presented in **Error! Reference source not found.**, to address the main questions emerging from this study on edge computing and descriptive, predictive, and prescriptive risk analytics.

Elements of artificial intelligence and machine learning in cognition engine design

Cyber risk analytics at present is reactive and assessments are based on risk/loss events that already occurred. AI/ML in forward-looking predictive analytics enable threat intelligence prediction and faster attack detection. The main advantage of AI in risk analytics is the fast processing and analysis of big data where parsing, filtering and visualisation is done in near real time. Machine learning uses mathematical and statistical methods and algorithms that learn, build and improve models from data. This enables design of a cognition engine in the form of automated predictive cyber intelligent software agents that identify, assess and record cyber-attacks. After this, natural language processing (NLP) can be applied to perform behaviour analytics and create baseline profiles of normal behaviour and then monitor for abnormalities while continuously learning from the profile's behaviour patterns. Facilitating a consistent and repeatable detection of threat indicators and predictions about new persistent risks that are undetected. AI/ML learn from multiple patterns (e.g. threat intelligence feed, device event logs, vulnerability information, contextual data) to determine predictive risk insights. Predictive risk analytics for advance notice of risk exposure and potential loss can be performed through monitoring the risk lifecycle activities, e.g. the reactive activities that

 doi:10.20944/preprints202003.0217.v1

capture losses and near miss events. From reactive activities we can quantify the impact of losses and develop baseline indicators to compare mathematical results.

Cognitive design

Connecting the lost exposure of cyber risk from human-computer interaction (frequency), in different information knowledge management systems (magnitude), with artificial intelligence, can provide predictive feedback sensors for primary and secondary loss (vulnerabilities). These feedback sensors represent dynamic real time data mechanisms that assist and enable better understanding of the vulnerabilities - prior to cyber-attacks. The reliability of cyber risk analytics could increase significantly if decisionmakers have a dynamic and self-adopting AI enhanced feedback sensors to assess, predict, analyse and address the economic risks of cyber-attacks.

Discussion

The novelty of the proposed research is in the relationship between AI/ML and securing the edge. With this study, we focused on delivering a higher Technology Readiness Level (TRL) by testing and verifying the formulae for risk analytics with industry actors in the field of AI/ML. The output of the research exhibits how an integration for dynamic real-time cyber risk analytics would work in industry settings. In addition, the research covers intersections between technology, regulation, economics, and interventions. This creates value across risk and engineering disciplines and resolves a contemporary problem that is relevant to the industry in general. Calculating the impact of cyber risk at the edge, with cyber risk analytics supported by AI/ML, contributes to cybersecurity of devices and networks at the edge. Therefore, the research relates to key government and industry priorities and end user needs.

This research addresses the need for improving our capacity for a comprehensive and systematic understanding of the opportunities and threats that arise when AI/ML technologies are migrated to the periphery of the internet and into local IoT networks. The research methodology approach was developed upon past experiences in terms of the (un)availability of data. Many similar models have been introduced and never used because reliable data could not be found. Furthermore, in terms of the (un)availability of data, lessons can be learned from previous research on data strategies [39]. The volume of data generated creates diverse challenges for developing data strategies in a variety of verticals (ex. AI/ML, ethics, business requirements). Simultaneously, designing a cyber security architecture for complex coupled systems, while understanding the economic impact, demands data strategy optimisation and decision making on collecting and assessment of probabilistic data when edge computing nodes are deployed, presents a socio-technical research problem.

The research is also strongly related to personal perceptions of risk because of collecting probabilistic data at the edge interact with data regulations, standards and policies. These data perceptions, regulations and policies are strongly considered in our approach for integrating AI/ML in cyber risk data analytics at the edge. A cybersecurity architecture for impact assessment with AI/ML cyber risk analytics must meet public acceptability, security standards, and legal scrutiny. With consideration of the above, the research integrated areas such as economic impact modelling, policy and governance recommendations with computer science, to develop and design architectures for AI/ML in cyber risk data analytics. The research contributes to knowledge by integrating economic impact assessment with AI/ML and cyber risk analytics models that have not been previously integrated for securing the edge, and thus promote the field of developing a dynamic and self-adopting AI enhanced data analytics methodology to assess, predict, analyse and address the economic risks of cyber-attacks.

Conclusion

With the integration of AI/ML in risk analytics at the periphery, and with the integration of IoT systems, it is only a question of time when AI/ML will start collecting and analysing risk data from IoT systems. With the rapid expansion of IoT systems at the periphery, the accompanying cyber risk will inevitably increase and the reliance on existing cyber risk metrics cannot be taken for granted when different and novel threat level emerges. This research concludes that impact assessment approaches need to be reconsidered and redesigned to include dynamic and self-adopting predictive cyber risk analytics. The conclusion builds upon the existing approach for categorising (pooling) risk, but presents a quantitative version of the NIST 'traffic lights' system (in **Error! Reference source not found.**), enhanced with multiple risk calculation metrics that calculate the shortfall probability, expected shortfall, VaR and CTE for different cyber risk levels and tail risk under different assumptions. This study enhances the Technology Readiness Level by presenting a mathematical formula for the future cyber risk developments that are reshaping not only the business ecosystems, but also the data analytics of supply and control systems. However, the AI/ML infrastructure in the communications network and the relevant cyber security technology must evolve in an ethical manner that humans can understand, while maintaining maximum trust and privacy of the users. IoT networks represent complex coupled systems [40], that can be described as cyber-physical social machines [41] and social machines [42] should be observed in practice [43]. Given that IoT is considered as critical enabler [44] of value creation [45], the findings of this study would probably be best verified when observed in practice.

Acknowledgment: The paper builds upon the foundation of existing knowledge developed from three PETRAS projects [46]–[48], but with a specific focus on Artificial Intelligence and Machine Learning (AI/ML) in IoT risk analytics. It benefits from the already established research knowledge, but with a focus on the topic of securing the edge through AI/ML real time analytics. To avoid overlapping with earlier work, this article avoids many relevant areas that have been addressed in the working papers and project reports that can be found in pre-prints online [49], [50], [59]–[64], [51]–[58].

References

[1] Chen, Zhuang., He, Qian., Liu, Lei., Lan, Dapeng., Chung, Hwei Ming., and Mao, Zhifei, "An artificial intelligence perspective on mobile edge computing," in *Proceedings - 2019 IEEE International Conference on Smart Internet of Things, SmartIoT 2019*, 2019, pp. 100–106.

[2] Tortora, Cristina., McNicholas, Paul D., and Palumbo, Francesco, "A Probabilistic Distance Clustering Algorithm Using Gaussian and Student-t Multivariate Density Distributions," *SN Comput. Sci.*, vol. 1, no. 2, pp. 1–22, Mar. 2020.

[3] Rahman, Mohammad S., and Haffari, Gholamreza, "A Statistically Efficient and Scalable Method for Exploratory Analysis of High-Dimensional Data," *SN Comput. Sci.*, vol. 1, no. 2, pp. 1–17, Mar. 2020.

[4] Latvala, Sampsa., Sethi, Mohit., and Aura, Tuomas, "Evaluation of Out-of-Band Channels for IoT Security," *SN Comput. Sci.*, vol. 1, no. 1, pp. 1–17, Jan. 2020.

[5] Gabillon, Alban., Gallier, Romane., and Bruno, Emmanuel, "Access Controls for IoT Networks," *SN Comput. Sci.*, vol. 1, no. 1, pp. 1–13, Jan. 2020.

[6] Gyongyosi, Laszlo., and Imre, Sandor, "Secret Key Rate Adaption for Multicarrier Continuous-Variable Quantum Key Distribution," *SN Comput. Sci.*, vol. 1, no. 1, pp. 1–17, Jan. 2020.

[7] Kar, Udit Narayana., and Sanyal, Debarshi Kumar, "A Critical Review of 3GPP Standardization of Device-to-Device Communication in Cellular Networks," *SN Comput. Sci.*, vol. 1, no. 1, pp. 1–18, Jan. 2020.

[8] Rajakumaran, Gayathri., Venkataraman, Neelanarayanan., and Mukkamala, Raghava Rao, "Denial of Service Attack Prediction Using Gradient Descent Algorithm," *SN Comput. Sci.*, vol. 1, no. 1, pp. 1–8, Jan. 2020.

[9] Hernandez, Netzahualcoyotl., Lundström, Jens., Favela, Jesus., McChesney, Ian., and Arnrich, Bert, "Literature Review on Transfer Learning for Human Activity Recognition Using Mobile and Wearable Devices with Environmental Technology," *SN Comput. Sci.*, vol. 1, no. 2, pp. 1–16, Mar. 2020.

[10] Abdel Magid, Salma., Petrini, Francesco., and Dezfouli, Behnam, "Image classification on IoT edge devices: profiling and modeling," *Cluster Comput.*, pp. 1–19, Aug. 2019.

[11] NetScouts, "Dawn of the TerrorBIT Era NETSCOUT Threat Intelligence Report-Powered by ATLAS Findings from Second Half 2018," 2018.

[12] Davis, Matovu., Gilbert, Mugeni., Simon, Karume., Stephen, Mutua., and Gilibrays Ocen, Gilbert, "State of cyber security: the Ugandan perspective," *Int. J. Sci. Eng. Res.*, vol. 10, no. 4, pp. 713–724, 2019.

[13] FAIR, "FAIR Risk Analytics Platform Management," *FAIR-U Model*, 2020. [Online]. Available: https://www.fairinstitute.org/fair-u. [Accessed: 26-Dec-2017].

[14] Ruan, Keyun, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," *Comput. Secur.*, vol. 65, pp. 77–89, 2017.

[15] CRatE, "Petras - Impact of Cyber Risk at the Edge: Cyber Risk Analytics and Artificial Intelligence (CRatE)," *EPSRC*, 2020. [Online]. Available: https://petras-iot.org/project/impact-of-cyber-risk-at-the-edge-cyber-risk-analytics-and-artificial-intelligence-crate/. [Accessed: 17-Feb-2020].

[16] Maple, Carsten, "Security and privacy in the internet of things," *J. Cyber Policy*, vol. 2, no. 2, pp. 155–184, May 2017.

[17] Tanczer, L.M., Steenmans, I., Elsden, M., Blackstock, J., and Carr, M., "Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?," in *Living in the Internet of Things: Cybersecurity of the IoT*, 2018, p. 33 (9 pp.).

[18] Breza, Michael., Tomic, Ivana., and McCann, Julie, "Failures from the Environment, a Report on the First FAILSAFE workshop," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 48, no. 2, pp. 40–45, May 2018.

[19] Ghirardello, K., Maple, C., Ng, D., and Kearney, P., "Cyber security of smart homes: development of a reference architecture for attack surface analysis," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 45 (10 pp.)-45 (10 pp.).

[20] Anthi, Eirini., Williams, Lowri., Slowinska, Malgorzata., Theodorakopoulos, George., and Burnap, Pete, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019.

[21] Boyes, Hugh., Hallaq, Bil., Cunningham, Joe., and Watson, Tim, "The industrial internet of things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.

[22] Agyepong, Enoch., Cherdantseva, Yulia., Reinecke, Philipp., and Burnap, Pete, "Challenges and performance metrics for security operations center analysts: a systematic review," *J.*

Cyber Secur. Technol., vol. 4, no. 1, pp. 1–28, Dec. 2019.

[23] Safa, Nader Sohrabi., Maple, Carsten., Watson, Tim., and Von Solms, Rossouw, "Motivation and opportunity based model to reduce information security insider threats in organisations," *J. Inf. Secur. Appl.*, vol. 40, pp. 247–257, Jun. 2018.

[24] Anthi, E., Williams, L., and Burnap, P., "Pulse: an adaptive intrusion detection for the internet of things," in *Living in the Internet of Things: Cybersecurity of the IoT*, 2018, p. 35 (4 pp.).

[25] Craggs, Barnaby., and Rashid, Awais, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," in *2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, 2017, pp. 22–25.

[26] Anthonysamy, Pauline., Rashid, Awais., and Chitchyan, Ruzanna, "Privacy Requirements: Present & Future," in *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track (ICSE-SEIS)*, 2017, pp. 13–22.

[27] Van Kleek, Max., Binns, Reuben., Zhao, Jun., Slack, Adam., Lee, Sauyon., Ottewell, Dean., and Shadbolt, Nigel, "X-Ray Refine," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 2018, pp. 1–13.

[28] Nurse, Jason RC., Radanliev, Petar., Creese, Sadie., and De Roure, David, "Realities of Risk: 'If you can't understand it, you can't properly assess it!': The reality of assessing security risks in Internet of Things systems," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–9.

[29] Nurse, J., Creese, Sadie., and De Roure, David, "Security Risk Assessment in Internet of Things Systems," *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.

[30] Akinrolabu, Olusola., Nurse, Jason R.C., Martin, Andrew., and New, Steve, "Cyber risk assessment in cloud provider environments: Current models and future needs," *Computers and Security*, vol. 87. Elsevier Ltd, p. 101600, 01-Nov-2019.

[31] Radanliev, Petar., De Roure, David., Nicolescu, Razvan., Huth, Michael., Montalvo, Rafael Mantilla., Cannady, Stacy., and Burnap, Peter, "Future developments in cyber risk assessment for the internet of things," *Comput. Ind.*, vol. 102, pp. 14–22, Nov. 2018.

[32] Radanliev, Petar., De Roure, David., Cannady, Stacy., Mantilla Montalvo, Rafael., Nicolescu, Razvan., and Huth, Michael, "Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, no. CP740, p. 3 (9 pp.).

[33] Radanliev, Petar., De Roure, David., Nurse, Jason R.C., Nicolescu, Razvan., Huth, Michael., Cannady, Stacy., and Mantilla Montalvo, Rafael, "Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0," in *Living in the Internet of Things: Cybersecurity of the IoT*, 2018, p. 41 (6 pp.).

[34] Buith, Jacques, "Cyber Value at Risk in the Netherlands," 2016.

[35] FAIR, "What is a Cyber Value-at-Risk Model?," 2017. [Online]. Available: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model. [Accessed: 26-Dec-2017].

[36] Malhotra, Yogesh, "Cognitive Computing for Anticipatory Risk Analytics in Intelligence,

Surveillance, & Reconnaissance (ISR): Model Risk Management in Artificial Intelligence & Machine Learning (Presentation Slides)," *SSRN Electron. J.*, Feb. 2018.

[37] Porambage, Pawani., Kumar, Tanesh., Liyanage, Madhusanka., Partala, Juha., Lovén, Lauri., Ylianttila, Mika., and Seppänen, Tapio, "Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI BrainICU-Measuring brain function during intensive care View project ECG-based emotion recognition View project Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI," 2019.

[38] Barker, Kash., Lambert, James H., Zobel, Christopher W., Tapia, Andrea H., Ramirez-Marquez, Jose E., Albert, Laura., Nicholson, Charles D., and Caragea, Cornelia, "Defining resilience analytics for interdependent cyber-physical-social networks," *Sustain. Resilient Infrastruct.*, vol. 2, no. 2, pp. 59–67, Apr. 2017.

[39] Radanliev, Petar., Roure, David C. De., R.C. Nurse, Jason., Montalvo, Rafael Mantilla., Cannady, Stacy., Santos, Omar., Madox, La'Treall., … Maple, Carsten, "Future developments in standardisation of cyber risk in the Internet of Things (IoT)," *SN Appl. Sci.*, no. 2: 169, pp. 1–16, 2020.

[40] De Roure, D., Page, K.R., Radanliev, P., and Van Kleek, M., "Complex coupling in cyber-physical systems and the threats of fake data," in *Living in the Internet of Things (IoT 2019), 2019 page*, 2019, p. 11 (6 pp.).

[41] Madaan, Aastha., Nurse, Jason., de Roure, David., O'Hara, Kieron., Hall, Wendy., and Creese, Sadie, "A Storm in an IoT Cup: The Emergence of Cyber-Physical Social Machines," *SSRN Electron. J.*, Sep. 2018.

[42] De Roure, David., Hooper, Clare., Page, Kevin., Tarte, Ségolène., and Willcox, Pip, "Observing Social Machines Part 2," in *Proceedings of the ACM Web Science Conference on ZZZ - WebSci '15*, 2015, pp. 1–5.

[43] Shadbolt, Nigel., O'Hara, Kieron., De Roure, David., and Hall, Wendy, *The Theory and Practice of Social Machines*. Cham: Springer International Publishing, 2019.

[44] Lee, Boyeun., Cooper, Rachel., Hands, David., and Coulton, Paul, "Design Drivers: A critical enabler to meditate value over the NPD process within Internet of Things," in *4d Conference Proceedings: Meanings of Design in the Next Era. Osaka : DML (Design Management Lab), Ritsumeikan University*, 2019, pp. 96–107.

[45] Lee, Boyeun., Cooper, Rachel., Hands, David., and Coulton, Paul, "Value creation for IoT: Challenges and opportunities within the design and development process," in *Living in the Internet of Things (IoT 2019). IET, Living in the Internet of Things 2019, London, United Kingdom*, 2019, pp. 1–8.

[46] IAM, "Petras - Impact Assessment Model for the IoT (IAM)," *EPSRC*, 2018. [Online]. Available: https://petras-iot.org/project/impact-assessment-model-for-the-iot-iam/. [Accessed: 20-Feb-2020].

[47] CRACS, "Petras - Cyber Risk Assessment for Coupled Systems (CRACS)," *EPSRC*, 2018. [Online]. Available: https://petras-iot.org/project/cyber-risk-assessment-for-coupled-systems-cracs/. [Accessed: 20-Feb-2020].

[48] Radanliev, P., Nicolescu, R., De Roure, D., and Huth, M., "Harnessing Economic Value from the Internet of Things," London, 2019.

[49] Radanliev, Petar., De Roure, David., Nurse, Jason R.C., Montalvo, Rafael Mantilla., and Burnap, Peter, "Standardisation of cyber risk impact assessment for the Internet of Things

(IoT)," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, Mar. 2019.

[50] Radanliev, Petar., Charles De Roure, David., Nurse, Jason R C., Burnap, Peter., and Montalvo, Rafael Mantilla, "Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[51] Radanliev, Petar, "Cyber Risk Management for the Internet of Things," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[52] Radanliev, P., Roure, D De., Nurse, JRC., and Nicolescu, R, "Cyber risk impact assessment–discussion on assessing the risk from the IoT to the digital economy," *Univ. Oxford Comb. Work. Pap. Proj. reports Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent.*, 2019.

[53] Radanliev, Petar., De Roure, David Charles., Nurse, Jason R.C., Montalvo, Rafael Mantilla., Burnap, Pete., Roure, David Charles De., Nurse, Jason R.C., … Montalvo, Rafael Mantilla, "Design principles for cyber risk impact assessment from Internet of Things (IoT)," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[54] Radanliev, Petar., De Roure, Dave., Cannady, Stacy., Montalvo, Rafael Mantilla., Nicolescu, Razvan., and Huth, Michael, "Analysing IoT cyber risk for estimating IoT cyber insurance," in *University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre*, 2019.

[55] Radanliev, Petar, "CYBER RISK IMPACT ASSESSMENT," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[56] Radanliev, Petar, "Digital Supply Chains for Industry 4.0 Taxonomy of Approaches," *Univ. Oxford Comb. Work. Pap. p*, no. April, 2019.

[57] Radanliev, P., De Roure, D., Nicolescu, R., and Huth, M., "A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[58] Radanliev, Petar., De Roure, David., Nurse, Jason RC., Burnap, Pete., Anthi, Eirini., Ani, Uchenna., Maddox, Treall., … Mantilla Montalvo, Rafael, "Cyber risk from IoT technologies in the supply chain-discussion on supply chains decision support system for the digital economy," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[59] Radanliev, Petar., De Roure, Dave., Nurse, Jason R C., Nicolescu, Razvan., Huth, Michael., Cannady, Stacy., and Montalvo, Rafael Mantilla, "Cyber Security Framework for the Internet-of-Things in Industry 4.0," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[60] Radanliev, Petar., DeRoure, David., Nurse, Jason R.C., Burnap, Pete., Anthi, Eirini., Ani, Uchenna., Santos, Omar., and Montalvo, Rafael Mantilla, "Definition of Cyber Strategy Transformation Roadmap for Standardisation of IoT Risk Impact Assessment with a Goal-

Oriented Approach and the Internet of Things Micro Mart," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[61] Radanliev, Petar., De Roure, David., Maple, Carsten., Nurse, Jason R.C., Nicolescu, Razvan., and Ani, Uchenna, "Cyber Risk in IoT Systems," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.

[62] Radanliev, Petar., De Roure, David., Nurse, Jason R.C., Nicolescu, Razvan., Huth, Michael., Cannady, Stacy., and Mantilla Montalvo, Rafael, "New developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – future developments in the Industrial Internet of Things and Industry 4.0," Preprints, Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, Mar. 2019.

[63] Radanliev, Petar., Roure, Dave De., Nurse, Jason R.C. C., Nicolescu, Razvan., Huth, Michael., Cannady, Stacy., Montalvo, Rafael Mantilla., … Montalvo, Rafael Mantilla, "Cyber Risk impact Assessment - Assessing the Risk from the IoT to the Digital Economy," Preprints, Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, Mar. 2019.

[64] Radanliev, Petar., De Roure, David Charles., Nurse, Jason R.C., Montalvo, Rafael Mantilla., and Burnap, Pete, "The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises," Oxford, University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre, 2019.