Adversarial Evolution: Competing dynamics and reactive institutional forms in financial services ecosystem

Paolo Spagnoletti [1,2], Federica Ceci [3] and Andrea Salvi [2]

[1] *Department of Information Systems, University of Adger, Kristiansand, Norway*
[2] *Department of Business and Management, Luiss University, Rome, Italy*
[3] *Department of Economics and Management, G. D'Annunzio University, Pescara, Italy*

Abstract

In this paper we conceptually illustrate the adversarial evolution of cybercrime and cybersecurity operations in financial services ecosystem. Building upon the concept of organizational morphing and ecosystem formation, we aim to reconstruct the parallel and conflict-driven evolution of the bright and dark side of financial services. Firstly, we identify five phases from the late 90s to the post-2015 period that show the paired configuration in the morphing of the two opposing sides. Secondly, we propose a conceptual model for digital ecosystems evolution based on the mutual influence of conflicting actors. This paper is a first foundational work towards a broader instantiation of generativity through adversarial evolution of digital ecosystems.

Keywords [1]

Cybersecurity, Cybercrime, Ecosystems, Financial Services, Innovation

1. Introduction

Financial cybercrimes seek profit through misappropriation of value in the financial services ecosystem. Such misappropriation is carried out through the malicious use of digital technologies and it is substantiated into criminal activities such as ransomware and phishing [1], [2]. Therefore, malicious actors master and exploit digital technologies as vectors misappropriation of value. These processes are continuously evolving and produce new forms of cybercrime at an extremely fast pace. This is the output of what some authors called outlaw innovation [3]. As Huang et al [4] puts it "to combat cybercrimes in an effective way, we not only need to develop technical solutions to protect against attacks but also need to understand the structure of the business of underground cybercrime and its development".

To fully appreciate the complexity of the dark – and criminal – side of financial ecosystems one should take into account the effects of such activity onto the "bright side" and vis-à-vis the opportunity it offers. Criminal activities in this domain have proliferated over the last decades, thanks to the diffusion of online banking and the widespread usage of electronic transfers of financial resources [5]. To create a safeguard against these ever-mutating malicious actions, also the bright side have evolved, adopting a variety of tactics, techniques and procedures, both at operational and strategic level [6], [7].

This brief contribution extends the studies over the link between link between the evolution of cybercrime and cybersecurity institutions in a digital service ecosystem, i.e., the financial sector. We build upon the observation that there is a linkage between innovations in the bright and in the dark side [3] and we attempt to show how that produces "conflict-driven" evolution. We show how the reiterated contacts between the bright and dark side of an ecosystem results in observable changes in technical innovations and in the evolution of the institutional forms adopted by the actors. We therefore propose

[1]TASEC21 Post-conference proceedings, April 07–09, 2021, Italy
EMAIL: pspagnoletti@luiss.it (A. 1); f.ceci@unich.it (A. 2); asalvi@luiss.it (A. 3)
ORCID: 0000-0003-1950-368X (A. 1); 0000-0002-6998-8534 (A. 2); 0000-0002-3583-0114 (A. 3)


the two adversaries in financial services as drivers of organizational change, being their fate deeply intertwined and far from being independent from each other. In other words, "belligerents" need to keep a competitive edge over the adversaries accounting for variation in their counterparts.

Building upon the contribution by Rindova and Kotha [8], we conceptualize this reactive and adaptive behavior as a process of continuous morphing. The determinants of such process are both systemic conditions and results of events instantiated in the digital ecosystem, where actors operate and mutate to match the shifting market conditions. That is: (1) bright and dark actors use morphing to keep a competitive edge in their environment; (2) the effects of their competition for appropriation/misappropriation of value results in changes in the ecosystem as a whole. As regard to the first point, we look at the institutional forms in these opposing domains proposing that they can capture structural changes and responses [9] of bright and dark actors modifying their value appropriation/misappropriation paths. We rely on an integrated view that suggests how the aforementioned tension (i.e. the conflicts between dark and bright actors) shapes the continuous morphing of institutional forms in digital ecosystems [10]. Having observed that co-evolution, we argue that Cybercrime and Security Operations (SecOp) are conflicting rather than complementary practices, both playing a role in digital ecosystems formation and evolution. Thus, the mutual influence of dark and bright actors shapes organizational morphing in digital ecosystems and a structural morphing of the same environment whereby they compete. Therefore, we elaborate a two-fold research questions: How data, technologies and actor configurations co-evolve in digital ecosystem? How Cybercrime and SecOp influence financial service ecosystem formation?

Firstly, we reconstruct and present the parallel and mutually influenced evolution of the bright and dark side. We accomplish that focusing on the practices of the two side to highlight how competing actors - engaging in the same ecosystem – reactively adapt their value-creation paths taking an institutional form that aim to counter the practices of the adversaries and "exploit" evolving systemic features. Secondly, we elaborate a conceptual model to explain how Cybercrime and SecOp drive evolution and morphing in a digital service ecosystem. Finally we present a brief illustrative case based on the financial services ecosystem. The case is built on a five-steps process from the late 90s to the post-2015 period.

2. Institutional forms and competition in digital service ecosystem

The digital service ecosystem is intended as the ensemble of "synergies and complementarities achieved between the activities, resources or outputs of several organizations" [10]. A specific form of digital service ecosystem is represented by the financial service ecosystem, that includes among others: banks, financial institutions, and LEAs. The financial service ecosystem witness competing activities and organizing of two counterparts: "bright" actors - in the form of legitimate organizations operating in the environment – and "dark" actors - broadly defined as outlaw users [3]. In this context, cybercriminals and SecOp constitute the "warring parties" of these two organizations. The tension between the two groups originates in colliding goals of appropriation and misappropriation of value, taking place in the environment in which they operate. In the security domain, few studies have been looking at the effect of deterrence generated by legislation and institutions [11]. Hui et al. (2017) estimate the effect of the Convention on Cybercrime on cyber-attack suggesting that – despite its merits – cybercriminals may adapt to these countermeasures and divert their attention to non-enforcing countries. This portrays dark actors as adaptable entities that can adjust their behaviors not only based on the feature of their environment, but also reacting to their "foes".

The open-ended nature of digital ecosystem, offers "dark" actors new opportunities to capture value through deception [13] and to allocate their resources more fluidly [14]. The growth of cyber threats shows that digital resources can serve as enabling tools for value misappropriation. Again, the process of misappropriation is hardly static: cybercriminals have been evolving over time at the individual levels and in their institutional forms. There has been a progressive professionalization of "hackers" [3]: they departed from the original connotation of "modders" or "product hackers" which characterized

the first wave of the phenomenon. Said evolution most likely depended in first place by the opportunities offered by the environment in which they operated. Yet, it became soon after a by-product of reactive behavior to opposing actors. In first place, resilience of criminal organizations carries over from "offline" instances crime [15]. Secondly, studies on organizational forms of cybercrime – such as the ones on Online Black Markets (OBMs) – have shown a high level of resilience of these platforms vis-à-vis the intervention of LEAs (Spagnoletti et al. 2018). The dark side is in fact particularly able to adapt and overcome challenges by re-organizing benefitting from its "less institutionalized" nature. This feature is embodied by a continuous morphing of institutional forms and organizational arrangements of malicious actors [17].

The literature shows the birth, the evolution and the end of bright and dark actors organising under different perspectives, but to date few frameworks consider their interplay and the effect on value creation at ecosystem level. In this paper, we show a five stages model **(Figure 1)** that depicts the co-evolution of cybercrime and cybersecurity institutions in financial ecosystems. We illustrate the validity of the model by presenting in the bright side the EU-OF2CEN (European Union Online Fraud Cyber - Center Expert Network) case, a public-private partnership aimed at contrasting financial cybercrime. In the dark side, on the same timeframe, between 2010 and 2015, we observed the evolution of carding in Online Blackmarkets (OBMs).

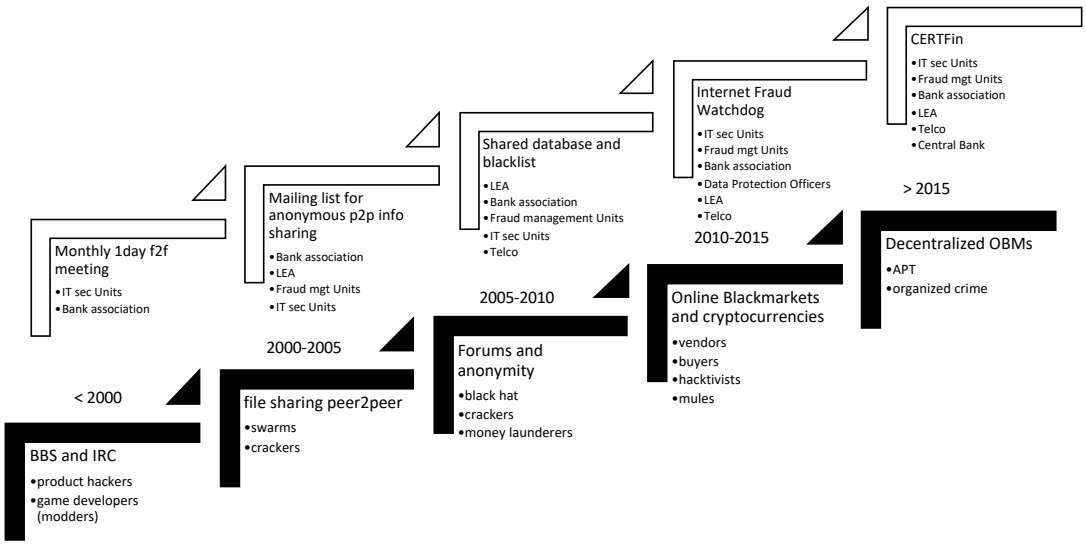

Figure 1: Co-evolution of institutional forms in bright and dark side of financial services ecosystems.

3. Illustrative case: OF2CEN and OBMs

The EU-OF2CEN – launched in 2013 - is an online platform that collect in real time, through secure communication channels, reports from banks and police on suspicious transactions that take place on the Internet, analyze them and share all information with the aim of identifying and blocking illegal operations. The platform allows the detection and sharing, through a system of "early warning" of reports related to possible criminal activities in progress. The project was conceived by the Italian Police, managed by Polizia Postale Department and financed by the European Union. For financial institutions, the birth of such platform translates into a significant increase in the ability to assess bank movements and into the subsequent implementation of effective actions to prevent or contain fraud or money laundering [18]. For Law Enforcement Agencies (LEAs), the aggregated analysis of the data collected can be used in structured investigative activities to enable more prompt attempts to recover from crime and facilitate the identification of responsible. The objectives of the platform are twofold: from a strategic viewpoint, the creation of a Public Private Partnership between Europol, LEAs and banks, favors the increase of common awareness about the modus operandi and criminal trends related

to financial cybercrimes, improving cooperation in the action of prevention and contrast; from an operational viewpoint, the sharing of relevant data allows to increase the ability to evaluate financial transactions carried out with the use of electronic tools, at national and international level. This facilitates concrete and timely actions to prevent and counter the recurrence of financial cybercrime. Therefore, in the OF2CEN we observe: (i) collaboration between IT security units and fraud management units; (ii) involvement of LEAs and information sharing between private and public actors; (iii) more capillary monitoring over transactions with prompter multi agency communications; (iv) refinement in shared data for anti-fraud.

As for the dark side, the timeframe between 2010 and 2015 embodies the raise and growth of OBMs. These platforms allowed for a series of low-risk, high-profit criminal activities (i.e. carding) that offered relatively easy value misappropriation paths for cyber-criminals in the financial ecosystem. These platforms encompass a wide variety of actors including hackers, site administrators, buyers, vendors and undercover LEA's agents. One of the main categories of digital goods pertaining the financial ecosystem listed in OBMs are credit cards details often referred to as "carding". It represents a major threat for businesses in all industrial sectors (Kraemer-Mbula et al. 2013; Spagnoletti et al. 2018). The phenomenon has evolved over time and OBMs enabled a series of incentives and technical solutions to make these activities low-risk and high-rewarding.

Our analysis of offers published between 2011 and 2016 in the category "digital goods" of major OBMs, shows that credit card numbers are sold in a variety of ways and with many additional services. Most vendors offer services to check the validity of the cards and commit to replace them based on the checker's result. Other vendors offer packages that guarantee the credit and spending balance. Others sell credit cards templates and holograms. Half of the offers are related to guides and tutorials explaining how to steal credit card information and how to use stolen cards minimizing the risk of being detected. The trade of illegal goods is conducted through anonymous transactions and shipping, guaranteed by the use of Tor network. The offer includes the display of goods, customer rankings of vendors, payment system (cryptocurrencies such as Bitcoin), and escrow functions, similar to those available in conventional e-commerce websites, for secure exchange. To build trust, buyers are called to rate vendors. Trust is central for OBMs, as we can see from the buyer's guidelines reported in one OBM:

"First of all, all members are kindly asked to be honest regarding package, delivery, product quality and shipping conditions. This helps maintaining a trusted network, which is a major basis in hidden web marketplaces. Scammers are not tolerated and are quickly identified as such" (http://xsuee6v24g2q6phb.onion/ help accessed on Dec 03, 2018).

Therefore, in the case of carding in OBMs referring to of our model we observe: (i) evolution of platforms to end to end services; (ii) collaboration and communication between an array of malicious actors: hackers, vendors, figureheads; (iii) more capillary and complex services and technological functionalities; (iv) refinement in data for financial fraud

4. Conceptual Model

A digital service ecosystem emerges around specific, value-reinforcing activities and resource complementarities [10]. What we know from the literature on ecosystems[2] and morphing [8] reconstruct an evolutionary pattern of digital ecosystem as driven by shifts in the market that lead actors to re-adjust their value-path. As shown in **Figure 2**, actors tend to come together achieving specific and value-reinforcing complementarities [21]. As time passes, external stimuli – e.g., in the form of technological changes – create a shift in market conditions within the ecosystem (marked with the dashed line). Therefore, actors will adjust their value-generating paths – which translates in new strategies and practices - leading to the emergence of new institutional forms. A new change in market conditions posits the need for further adjustments that occur within the digital service ecosystem, at that

[2] See [10] for an extensive review.

point new actors (e.g., A4) with a value driven interest in the ecosystem may join the digital service ecosystem. Conversely, actors whose value-generating paths do not align with the new shift in market condition may opt-out (e.g., A2).

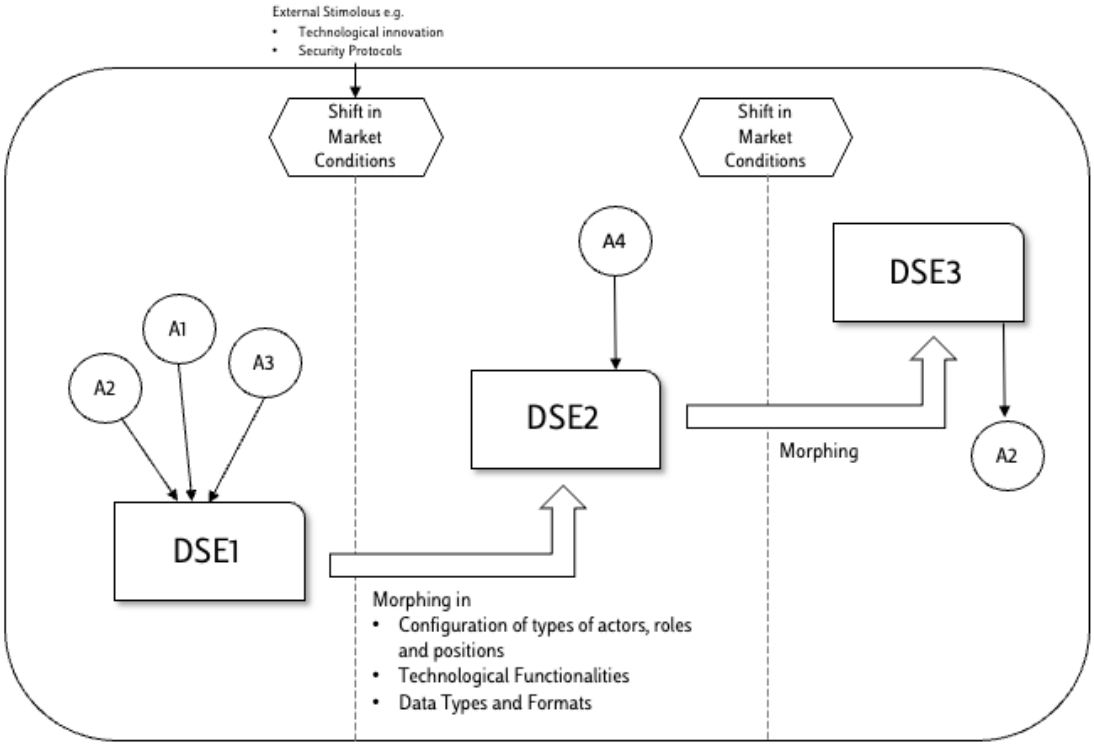

Figure 2: Market-driven changes in digital ecosystem and generation of new institutional forms over time.

The limit of this model is that it only reflects changes as driven by systematic and exogenous changes but do not take into the account the interactions between conflicting members of the digital ecosystem. Here, we present a preliminary conceptual model able to grasp how conflicting dynamics can generate innovation within a digital ecosystem. These changes are therefore a by-product of a conflict-driven interaction between actors. As shown in **Figure 3**, actors are pushed to adjust their value generating paths not only by exogenous shocks but also due to shifts in competitive conditions with their counterparts. In other words, competing for appropriation/misappropriation of value create a feedback that influences adjustment in value-driven paths resulting in adversarial institutional forms. We argue that the digital ecosystem will adjust accordingly to meet shift in market conditions and competitive conditions.

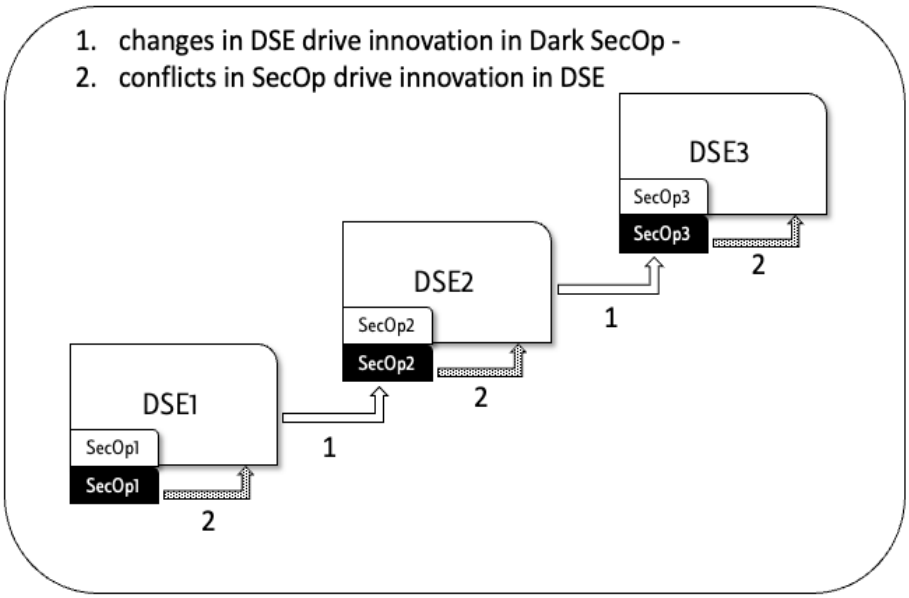

Figure 3: Basic representation of Adversarial Evolution of a digital ecosystem - Evolution as a result of conflict driven interactions between Dark and Bright SecOps.

5. Conclusion

In this brief contribution, we focus on one specific case of a digital ecosystem, the financial services ecosystem, to empirically analyze the co-evolution of institutional forms that emerge between conflicting actors (i.e., cybercriminals and legal actors). Firstly, we identified five phases of co-evolution from the late 90s to the post-2015 period relying on secondary sources. From empirical observation, we proposed a the foundations of a conceptual model for digital ecosystems evolution based on the adversarial evolution. This contribution constitutes the first step towards a broader theoretical understanding of the generativity of opposing forces in digital ecosystem.

6. References

[1] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," *Inf. Manag.*, vol. 51, no. 1, pp. 138–151, Jan. 2014, doi: 10.1016/j.im.2013.11.004.

[2] D. Pienta, J. B. Thatcher, and A. Johnston, "Protecting a whale in a sea of phish," *J. Inf. Technol.*, vol. 35, no. 3, pp. 214–231, Jun. 2020, doi: 10.1177/0268396220918594.

[3] S. Flowers, "Harnessing the hackers: The emergence and exploitation of Outlaw Innovation," *Res. Policy*, vol. 37, no. 2, pp. 177–193, 2008, doi: 10.1016/j.respol.2007.10.006.

[4] K. Huang, M. Siegel, and S. Madnick, "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, 2018.

[5] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," *Eur. J. Crim. Policy Res.*, vol. 23, no. 3, pp. 287–300, 2017, doi: 10.1007/s10610-016-9332-z.

[6] A. Calderaro and A. Craig, "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building," *Third World Q.*, vol. 0, no. 0, pp. 1–22, 2020, doi: 10.1080/01436597.2020.1729729.

[7] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[8] V. P. Rindova and S. Kotha, "Continuous 'Morphing': Competing through Dynamic Capabilities , Form and Function," *Acad. Manag. J.*, vol. 44, no. 6, pp. 1263–1280, 2001, doi: 10.2307/3069400.

[9] G. Vial, "Understanding digital transformation: A review and a research agenda," *Journal of Strategic Information Systems*, vol. 28, no. 2. Elsevier B.V., pp. 118–144, Jun. 01, 2019, doi: 10.1016/j.jsis.2019.01.003.

[10] C. Alaimo, J. Kallinikos, and E. Valderrama, "Platforms as service ecosystems: Lessons from social media," *J. Inf. Technol.*, vol. 35, no. 1, pp. 25–48, Oct. 2019, doi: 10.1177/0268396219881462.

[11] S. H. Kim, Q.-H. H. Wang, and J. B. Ullrich, "A comparative study of cyberattacks," *Commun. ACM*, vol. 55, no. 3, pp. 66–73, 2012, doi: 10.1145/2093548.2093568.

[12] K. Hui, S. H. Kim, and Q. Wang, "Cybercrime Deterrence and International Legislation: Evidence From Distributed Denial of Service Attacks," *MIS Q.*, vol. 41, no. 2, pp. 497-A11, 2017, doi: 10.14208/eer.2013.03.02.005.

[13] S. Grazioli and S. L. Jarvenpaa, "Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence," *Int. J. Electron. Commer.*, vol. 7, no. 4, pp. 93–118, 2003, doi: Article.

[14] Y. Wang, T. Stuart, and J. Li, "Fraud and Innovation," *Adm. Sci. Q.*, vol. 66, no. 2, pp. 267–297, Jun. 2020, doi: 10.1177/0001839220927350.

[15] S. Agreste, S. Catanese, P. De Meo, E. Ferrara, and G. Fiumara, "Network structure and resilience of Mafia syndicates," *Inf. Sci. (Ny).*, vol. 351, pp. 30–47, 2016, doi: 10.1016/j.ins.2016.02.027.

[16] P. Spagnoletti, F. Ceci, and B. Bygstad, "An investigation on the generative mechanisms of Dark Net markets," 2018.

[17] F. Ceci, A. Prencipe, and P. Spagnoletti, "Evolution, Resilience and Organizational Morphing in Anonymous Online Marketplace," *Acad. Manag. Glob. Proc.*, no. 2018, p. 62, 2018.

[18] P. Spagnoletti and A. Salvi, "Digital systems in High-Reliability Organizations: balancing mindfulness and mindlessness," in *Proceedings of the 6th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2020), June 8-9, 2020*, 2020, vol. 0114, no. Stpis, pp. 155–161, [Online]. Available: http://ceur-ws.org/Vol-2789/paper21.pdf.

[19] E. Kraemer-Mbula, P. Tang, and H. Rush, "The cybercrime ecosystem: Online innovation in the

shadows?," *Technol. Forecast. Soc. Change*, vol. 80, no. 3, pp. 541–555, 2013.
[20] P. Spagnoletti, G. Me, F. Ceci, and A. Prencipe, "Securing national e-ID infrastructures: Tor networks as a source of threats," in *Organizing for the Digital World. IT for individuals, communities and societies*, F. Cabitza, C. Batini, and M. Magni, Eds. LNISO - Springer, 2018, pp. 1–14.
[21] M. G. Jacobides, C. Cennamo, and A. Gawer, "Towards a theory of ecosystems," *Strateg. Manag. J.*, vol. 39, no. 8, pp. 2255–2276, 2018.