12-12-2020

THE BRIGHT AND DARK SIDE OF FINANCIAL SERVICES ECOSYSTEM

Paolo Spagnoletti

Federica Ceci

Andrea Salvi

THE BRIGHT AND DARK SIDE OF FINANCIAL SERVICES ECOSYSTEM

Paolo Spagnoletti
Department of Information Systems, University of Agder,
Kristiansand, Norway and
Department of Business and Management, Luiss University,
Rome, Italy

Federica Ceci
Department of Economics and Management, G. d'Annunzio University,
Pescara, Italy

Andrea Salvi[1]
Department of Business and Management, Luiss University,
Rome, Italy

In this brief contribution we focus on the co-evolution of cybercrime and cybersecurity practices in the banking and financial sector. We draw on previous studies on outlaw innovation and organizational morphing to reconstruct the parallel and mutually influenced evolution of the bright and dark side of financial services. We identify five phases from the late 90s to the post-2015 period that show the paired configuration in actors, techniques, collaborative actions, and venues in the morphing of the two opposing sides. This paper constitutes the first step towards a broader empirical analysis on the generativity of opposing forces in digital ecosystems.

Keywords: cybercrime, morphing, anti-fraud, cybersecurity

[1] Corresponding author asalvi@luiss.it

INTRODUCTION

Financial cybercrimes are profit-driven forms of crimes such as phishing and ransomware attacks aimed at misappropriating value through the malicious use of digital technologies (Baskerville et al. 2014; Pienta et al. 2020). Malicious actors harness and exploit digital technologies aiming for the sake of misappropriation of value, producing a set of new forms of cybercrime as the results of an outlaw innovation process in the dark (Flowers 2008). Financial cybercrimes considerably affect the bright side of the banking and financial sector. In fact, such criminal practices have become increasingly problematic over the last 25 years, with the advent of online banking and the proliferation of electronic funds transfer systems (Leukfeldt et al. 2017). To protect banks and financial services' customers from the threat of cybercrime, cybersecurity practices are performed by multiple actors at different levels of the bright side (Calderaro and Craig 2020; Von Solms and Van Niekerk 2013).

In this brief contribution we investigate the existence of a link between the evolution of cybercrime and cybersecurity institutions in the banking and financial sector. As proposed by Flowers (2008), there is a linkage between innovations in the bright and in the dark side. Here, we argue that this linkage is not solely observable in technical innovation, but also in the evolution of institutional forms. In simple terms, drivers of organizational change of the two sides of financial services are hardly independent from each other as they need to account for the variations in the counterparts. We frame this reactive behavior of adaptation as a form of continuous morphing (Rindova and Kotha 2001) driven by systemic conditions and instantiated in the digital ecosystem where actors operate and mutate to match the shifting market conditions.

In short, bright and dark actors use morphing to keep a competitive edge in their environment. We look at the institutional forms in these opposing domains proposing that they can capture structural changes and responses (Vial 2019) of bright and dark actors modifying their value appropriation/misappropriation paths. In this paper, we offer a first example of an integrated view that suggests how the aforementioned tension shapes the continuous morphing of institutional forms in digital ecosystems (Alaimo et al. 2019). Therefore, our research question is: how cybercrime and cybersecurity institutions co-evolve in financial services ecosystems?

To reconstruct the parallel and mutually influenced evolution of the bright and dark side, we focus on information security and financial cybercrime practices respectively. This choice illustrates how competing actors who share the same ecosystem forge their value-creation paths in a reactive fashion and adopt institutional forms that best fit two stimuli: (1) counterparts' practices and (2) evolving systemic features (including technologies and their constraints). We identify five phases from the later 90s to the post-2015 period that show the paired configuration in actors, techniques, collaborative actions and venues in the morphing of the two opposing sides.

INSTITUTIONAL FORMS IN THE BRIGHT AND DARK SIDE OF FINANCIAL SERVICES ECOSYSTEM

The financial service ecosystem witness the 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 cybercriminals or outlaw users (Flowers 2008). 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 (Kim et al. 2012). 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 infrastructures, offers "dark" actors new opportunities to capture value through deception (Grazioli and Jarvenpaa 2003). 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" (Flowers 2008): 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 (Agreste et al. 2016). 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 (Paolo 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 (Ceci et al. 2018).

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 develop 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 partnerships 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).

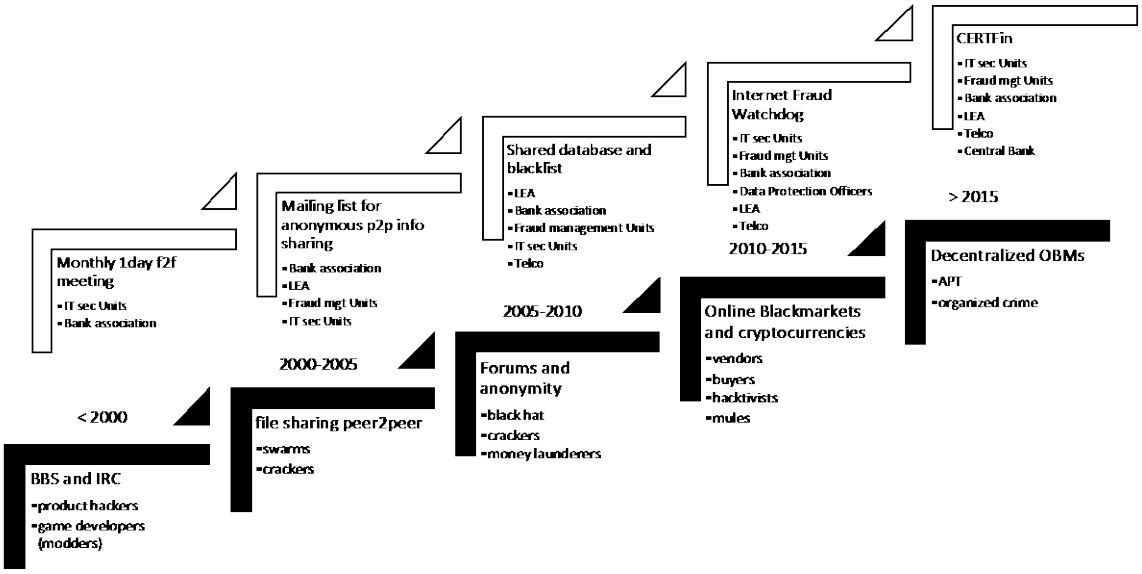

Figure 1 – Co-evolution of institutional forms in bright and dark side of financial services ecosystems

ILLUSTRATIVE CASE: OF2CEN AND CARDING IN 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 (Spagnoletti and Salvi 2020). 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

CONCLUSION

In this contribution, we focus on the financial services ecosystem to empirically analyze the co-evolution of institutional forms that emerge between cybercriminals and legal actors. This contribution constitutes the first step towards a broader theoretical understanding of the generativity of opposing forces in digital ecosystems.

REFERENCES

Agreste, S., Catanese, S., De Meo, P., Ferrara, E., and Fiumara, G. 2016. "Network Structure and Resilience of Mafia Syndicates," *Information Sciences* (351), Elsevier Inc., pp. 30–47.

Alaimo, C., Kallinikos, J., and Valderrama, E. 2019. "Platforms as Service Ecosystems: Lessons from Social Media," *Journal of Information Technology* (35:1), SAGE Publications Ltd, pp. 25–48.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," *Information & Management* (51:1), Elsevier B.V., pp. 138–151.

Calderaro, A., and Craig, A. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building," *Third World Quarterly* (0:0), Routledge, pp. 1–22.

Ceci, F., Prencipe, A., and Spagnoletti, P. 2018. "Evolution, Resilience and Organizational Morphing in Anonymous Online Marketplace," *Academy of Management Global Proceedings* (2018), Academy of Management Briarcliff Manor, NY 10510, p. 62.

Flowers, S. 2008. "Harnessing the Hackers: The Emergence and Exploitation of Outlaw Innovation," *Research Policy* (37), pp. 177–193.

Grazioli, S., and Jarvenpaa, S. L. 2003. "Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence," *International Journal of Electronic Commerce* (7:4), pp. 93–118.

Hui, K., Kim, S. H., and Wang, Q. 2017. "Cybercrime Deterrence and International Legislation:

Evidence From Distributed Denial of Service Attacks," *MIS Quarterly* (41:2), pp. 497-A11.

Kim, S. H., Wang, Q.-H., and Ullrich, J. B. 2012. "A Comparative Study of Cyberattacks," *Communications of the ACM* (55:3), ACM New York, NY, USA, pp. 66–73.

Kraemer-Mbula, E., Tang, P., and Rush, H. 2013. "The Cybercrime Ecosystem: Online Innovation in the Shadows?," *Technological Forecasting and Social Change* (80:3), pp. 541–555.

Leukfeldt, E. R., Lavorgna, A., and Kleemans, E. R. 2017. "Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," *European Journal on Criminal Policy and Research* (23:3), European Journal on Criminal Policy and Research, pp. 287–300.

Pienta, D., Thatcher, J. B., and Johnston, A. 2020. "Protecting a Whale in a Sea of Phish," *Journal of Information Technology* (35:3), SAGE Publications Ltd, pp. 214–231.

Rindova, V. P., and Kotha, S. 2001. "Continuous 'Morphing': Competing through Dynamic Capabilities , Form and Function," *Academy of Management Journal* (44:6), pp. 1263–1280.

Von Solms, R., and Van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers and Security* (38), Elsevier Ltd, pp. 97–102.

Spagnoletti, Paolo, Ceci, F., and Bygstad, B. 2018. "An Investigation on the Generative Mechanisms of Dark Net Markets," in *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy*.

Spagnoletti, P., Me, G., Ceci, F., and Prencipe, A. 2018. "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, pp. 1–14.

Spagnoletti, P., and Salvi, A. 2020. "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*, CEUR Workshop Proceedings (CEUR-WS.org).

Vial, G. 2019. "Understanding Digital Transformation: A Review and a Research Agenda," *Journal of Strategic Information Systems*, Elsevier B.V., pp. 118–144.