Chapter 46
Social Research Methods in Cybersecurity:
From Criminology to Industrial Cybersecurity

Felix Antonio Barrio
https://orcid.org/0000-0002-1660-0479
University Isabel I de Castilla, Spain

Raquel Poy
University of Leon, Spain

ABSTRACT

The application of social research methods in cybersecurity requires a multidisciplinary combination since the security of technologies and communication networks is made up of a set of uses, techniques, and results directly conditioned by the parameters of confidentiality, data availability, integrity, and privacy. However, each of these technological concepts is prepared and subject to conditions of use that involve ethical, sociological, economic, and legal aspects. Firstly, social engineering techniques in cybercrime tend to combine social investigation techniques with computational engineering and telecommunications elements. Secondly, research on cybersecurity phenomena in industrial environments implies the adaptation to the organizational specificity of each sector. In this chapter, the social research topics commonly addressed by leading companies and researchers in cybersecurity at a global level are analyzed from a comparative point of view, extracting a taxonomy of social research on cybersecurity.

INTRODUCTION

Universal access to Information and Communication Technologies (ICT) and, significantly, global access to the Internet have increased our dependence on the normal functioning of accesses, data manipulation, and transmission of data. It is unnecessary to point out how this dependency has reached critical values for people or organizations. Consequently, we must be aware that security has become a substantial ele-

DOI: 10.4018/978-1-7998-8473-6.ch046

ment of the digital society and economy. As Ulrich Beck anticipated in the 1980s, the growing social concern about the risks humans had created made the risk of new technologies one of the main interests in the social sphere (Beck, 1992). The 'risk society' predicted by Beck was becoming a reality in the 'digital society' (Lupton, 2016). Beck, Castel, or Luhmann led the sociological analysis of the end of the past century on uncertainty and fear of risk (Castel, 1991; Luhmann et al., 2017). These authors stand out in a broad theoretical movement that puts the concept of risk at the center of sociological theory (Adam *et al*., 2000). This debate highlights the relationships between concepts such as risk, technology, social communication, or uncertainty management. As a whole, this debate allows us to verify that our post-industrial society has had an accelerated dependence on technology in recent decades, notably represented by cybersecurity.

COVID-19 pandemic has boosted the consumption of digital services, including remote working or education and electronic leisure, pushing consumption patterns that will consolidate to a great extent among users even after the recovery of normality (Ting *et al*., 2020; Papadopoulos *et al*., 2020). But the displacement of traditional consumption and economic activity to the digital world also drives the motivations of attraction to cybercriminals, whose guidelines for action have become more sophisticated (Lallie *et al*., 2021).

Cybersecurity is an area of technological risk management that combines purely technical aspects with behavioral issues about how people use information and communication technologies regarding confidentiality, integrity, and data availability. Otherwise, the fact that 95% of the technological risks related to suffering a cyberattack by cybercriminals 'are human-enabled' (Nobles, 2018), implies that the relevance of social research has had exponential growth in the last decade.

Given this perspective, the importance acquired by the social study of cyber risks is understood, which has only recently received the necessary academic recognition. The existence of a disciplinary field such as cybersecurity barely acquired a birth certificate a decade ago. In 2010 the MITRE corporation commissioned the JASON Advisory Group to write a report on a possible scientific disciplinary area named cybersecurity. The group of experts linked the successful development of the new discipline to the joint effort of an academic, industrial, and laboratory network that should feed with knowledge an authentic research body (JASON, 2010: 6-7). Although initially, they conferred a secondary role to the social sciences, they recognized that their observational methods should establish synergies with those based on the technological field. But social research had already begun its journey within the framework of studies promoted by specialized companies and government agencies with interests in this field, establishing two different lines of work.

In the last decade, large consulting firms such as Gartner or Forrester and multinationals such as Microsoft, IBM, Cisco, Deloitte, or Accenture, which have developed business divisions specialized in the research, have monopolized knowledge production on cybersecurity. This fact is part of a corporative strategy to maintain the necessary competitiveness within the framework of the technology industry. (Walton et al., 2021). Often in collaboration with academia, these research centers have proven essential to contribute to the generation of research on risks and threats and their impact on society and the economy at a global and regional level. However, they are not exempt, as we will see, from the controversy over their possible biases in impartiality (Maschmeyer *et al*., 2021).

On the other hand, the role in social research of government agencies as the reference centers for cybersecurity in developed countries has proven fundamental to promote cybersecurity research about public issues. Although enabling different regulatory and strategic frameworks, American, European, and Australian institutions have strategic research agendas to consider (Wang *et al*., 2016).