The advent of the Internet and the diffusion of computer technologies worldwide have resulted in an unprecedented global expansion of computer-based criminal activity. The very nature of these attacks is also shifting from traditional cybercrime involving lone hackers targeting monolithic entities to involvement of organized crime groups. In the past hackers may have attacked for fun, notoriety, or to challenge themselves, while financial motivations are major consideration nowadays. Computer criminals have begun deploying advanced distributed techniques, which are increasingly effective and devastating. The aim of this mini-track is to encourage research that provides insights into the issue of cybercrime in the digital economy. The six papers included in this mini-track reflect this goal.

Hu, Zhang and Xu, in their paper, “Moral Beliefs, Self-Control, and Sports: Effective Antidotes to the Youth Computer Hacking Epidemic” address the question why young computer talents become computer hackers. The authors focus on past experience, routine activities, moral beliefs, and self-control characteristics of individual subjects to understand how talented computer savvy college students may become computer hackers. The aim of their study is to identify and confirm the factors that contribute to the evolution of computer hackers.

Watters, Layton and Dazeley, in their paper “How much material on BitTorrent is infringing content? A case study”, propose a new observational methodology for measuring the extent of infringing content. The researchers focus on BitTorrent, which is a widely used protocol for peer-to-peer (P2P) file sharing, to measure the true extent of illegal file sharing. The intent of the authors is to understand the actual scale and scope of the problem of digital piracy.

Reardon, Nance and McCombie, in their paper “Visualization of ATM Usage Patterns To Detect Counterfeit Cards Usage”, focus on card-present fraud involving Automated Teller Machine (ATM). This paper demonstrates the value of visualization to detect ATM usage anomalies including skimmed (counterfeited) card fraud. The authors argue that visualization techniques, coupled with human abductive reasoning, can be effective in detecting card related cybercrime.

Unethical IT use is another aspect of cybercrime. In the paper “Unethical Use of Information Technology: A Two-Country Study”, Chatterjee, Valacich and Sarker propose an integrative model of factors that influence individuals’ unethical use of IT. The researchers test their model among young adult participants in USA and Finland. The study emphasizes how ethical theories from philosophy can inform our understanding of unethical IT use and how IT plays a role in facilitating unethical behavior.

Online harassment in anonymous cyberspace is a real issue. It is yet another facet of cybercrime. In the paper “Empirical Analysis of Online Anonymity and User Behaviors: the Impact of Real Name Policy”, Cho, Acquisti and Kim examine the effectiveness of Internet regulation in terms of online privacy and anonymity. The focus of the study is on the Real Name Verification Law of South Korea, which was implemented in 2007. The intent of this regulation was to make user identity traceable by requiring online users to verify their real identity. The researchers investigate whether this regulation had any impact on uninhibited online behavior.

Tejay and Zadig, in their paper “Investigating the Effectiveness of IS Security Countermeasures Towards Cyber Attacker Deterrence”, examine the efficacy of current information system (IS) security countermeasures upon the deterrence of external cyber attackers. The authors argue that the deterrent effect of security countermeasures varies based upon two primary factors: whether they are deployed internally or externally to the organization; and whether the countermeasures actively prevent attacks or passively collect data on attacks for future action. This study uses data collected from hacker bulletin boards to understand the effects of IS security countermeasures upon the intentions of cyber attackers.

All these papers present important perspectives on cybercrime in the digital economy. Each paper touches upon a unique facet of cybercrime and contributes to the theoretical development of cybercrime and information security literature.