



IMSIS
International Master
Security, Intelligence
& Strategic Studies



**Erasmus
Mundus**

Friends, Rivals, Foes: The Private Sector and Online Vigilantism Impact on Police Cyber Capabilities

August 2021

University of Glasgow #: 2468006m

Dublin City University #: 19108682

Charles Prague University #: 75713277

**Presented in partial fulfilment of the requirements for the
Degree of
International Master in Security, Intelligence and Strategic Studies**

Word Count: 21,997

Supervisor: Prof. Oldrich Bureš

Date of Submission: August 2nd, 2021

Abstract

Cybercrimes and the evolution of new technologies have brought with them an expansion and change within the policing structures that govern cyberspace. Thus, the different nodes of governance in the virtual environment were broken down and identified; as per the scope of this



**University
of Glasgow**



CHARLES UNIVERSITY

research the key categories explored were law enforcement agencies, private industries, and online vigilantes. Questions pertaining to the regulatory scope and capabilities of these groups in cyberspace were then analysed, focusing on some clear links and connections that have previously been largely ignored by scholars, policy makers and other researching bodies.

The purpose of this research study was to demonstrate how the different nodes of governance work to achieve the deterrence what are considered of lower-tier cybercrimes. Different case studied were critically analysed to measure and develop understanding on why these different governance nodes are not successfully achieving the deterrence of cybercrime, identifying wherein changes need to be made to improve the future capabilities and capacity pertaining to the policing of cybercrimes. This study was grounded in the use of qualitative research methods used to examine the relationship between all these nodes of governance and their failings in deterring and policing cybercrimes.

The aim was to link general deterrence theory; which develops an understanding on the general requirements needed to ensure successful crime deterrence such as consistent, proportionate punishments to ensure that the risk of a crime outweighs the rewards; with the techniques, practices and processes of the police, the private sector, and online vigilantes.

Overall, the paper argues that to successfully deter cybercrimes these nodes of governance need to increase their cooperative measures to successfully achieve the technical knowledge and capacity to complete investigations and the authoritative power that can ensure the certainty of punishment. Clear recommendations were made to improve the deterrence capabilities of these different nodes of governance.