How industry can help us fight against botnets

Karine K. e Silva, Tilburg University

This paper canvasses industry participation as a viable means for an improved response to botnets. It examines the obstacles to private sector participation in countering botnets and how alternative forms of regulation can facilitate this participation. Botnets have been recurrently flagged as one of the most pervasive cybercrime infrastructures of our time. Used for launching powerful attacks, botnets generate income for their masters while harming millions of users. However, the tradition model of law enforcement has yielded poor results against them and attacks continue to grow in scale and impact.

Enforcing the rule of law against botnets has been a notoriously daunting task, evidenced by the wide contrast between statistics on bot infections and inflicted losses, on the one hand, and the low numbers of formal prosecution, on the other hand. Recent law enforcement operations have attempted to overcome these setbacks by calling for support from the private sector. Owing to their expertise and strategic infrastructure, industry is well equipped to tackle botnets in a way law enforcement cannot match. Private sector, in turn, may benefit from these operations by having a key opportunity to defend their networks, protect their customers, and strengthen their business model. As such, both governments and companies are keen to admit that businesses, not public authorities, are in a privileged position to timely detect, prevent, and react to botnets.

Nevertheless, industry participation faces important challenges. The promises that by involving the Internet industry nations will enhance their response to botnets stumble upon criticism over the viability and legitimacy of this hybrid model of law enforcement. The concerns about expanding industry participation include the lack of transparency and accountability of private sector activities, and the absence of sufficient incentives to ensure the companies will act on the public interest. In addition, even if considered as the crown jewel of botnet mitigation, the Internet industry may not possess the best information to decide on the lawfulness of countermeasures. Thus, private actors may also lack the means to adjudicate whether and under what circumstances they should respond to an attack.

Despite its advantages, private sector collaboration remains largely unregulated. As a result, unsolved issues of accountability, transparency, and legitimacy have hampered further public-private interaction. In order to increase regulatory certainty and advance industry support, this paper proposes a combination of three regulatory approaches that could shape future regulation on botnets. To this end, this study adopts a comparative legal research perspective. It looks at countries with a track record of public-private cooperation against botnets and how national regulators have been dealing with this challenge. Considering the effectiveness (as well as the lack thereof) of the framework enacted in the Netherlands and in a sample of jurisdictions (United States, Germany, and Finland), a hard law and two soft law mechanisms will be analyzed, based on the experiences of regulators and regulatees. These are legislation, sector guidelines, and sectorial codes of conduct, the applicability and implications of which are further explored in the paper.