Political Sciences

3rd International Conference on Political Sciences
18 - 20 July 2025
London, United Kingdom

Effects and Limitations of the Interaction between Public Attribution and Offensive Cyber Operations on Cyber Deterrence by Punishment Rethinking of the Risk of Retaliation

Akira Ichida

Keio University, Japan

Abstract

From the perspective of a cyber defender, the matter of dealing with cyberattacks is of the paramount importance. Nevertheless, the most efficient strategy to be adopted is one of prevention, i.e. the deterrence of cyberattacks before they occur. J. Nye describes deterrence as a psychological process that depends on the perceptions of both attacker and defender, and the ability to communicate these perceptions with clarity. In recent years, public attribution (PA) has become a prevalent and substantial method of articulating the defender's intentions. Nevertheless, the efficacy of PA in terms of cyber deterrence does not appear to exceed the anticipated level. Conversely, since 2016, the initiation of deployment of Offensive Cyber Operations (OCO) has been progressively disclosed to the public, along with the announcement of PA. This has compelled attackers and third parties contemplating or intending to attack to reassess the cost-effectiveness of doing so, thus raising the threshold for such actions. The paper therefore uses 2016 as a divided point of comparison, with the aim of clarifying the combination of OCO and PA to be effective. The study concludes that the effectiveness of cyber deterrence through punishment is beginning to be demonstrated in the context of states and state-sponsored hacker groups.

Keywords: communication; dissemination; implicit; intent; psychological