Policy Surveillance in the Field of Cybercrime Prevention: An Opportunity to move Beyond *ad hoc* Interventions (and to compare cyber apples to digital oranges)

Benoît Dupont

The statistics available on the volume and costs of cybercrime, however imprecise and fragmentary, are staggering. In 2014, the Center for Strategic and International Studies estimated that cybercrime and espionage costs $445 billion annually, which would roughly amount to 1% of global income. A more cautious and conservative assessment made by a team of computer scientists and criminologists from UK data suggests that the global cost of cybercrime around the 2010s reached $75 billion—and $225 billion if traditional crimes transitioning to cyber were included. As a result, government and business leaders have ranked cyber-risks at the top of their security concerns for the past few years and are investing heavily into cybercrime prevention and cybersecurity policies. Unfortunately, there is no source of consolidated data that would enable us to measure and track these efforts at the global and national levels, nor do we have a centralized database of the various policies and programs implemented by public, private and community stakeholders to manage those risks. This lack of information is problematic for three main reasons: 1) It prevents us from being able to systematically assess the nature, effectiveness and efficiency of the various policies that are being adopted across the world to prevent and control cybercrime; 2) At the international level, this lack of baseline information restricts the dissemination of knowledge and impedes the adoption of policies that have been proven to deliver positive outcomes, as well as preventing the debunking of failed or counterproductive policies. Beyond the lack of evaluation and sharing, the absence of a common framework to analyze policies also hinders coordination efforts that would deliver more effective responses to transnational cybercrime and cyber-risks. To answer these challenges and to overcome the knowledge gap they reflect, this presentation will discuss the feasibility of applying a policy surveillance methodology to map international cybercrime prevention efforts. Policy surveillance has been defined as "the systematic collection, analysis and dissemination of information about laws and other policies". After having introduced the five criteria of policy surveillance, its history in other policy areas will be examined. A discussion of existing cybersecurity policy monitoring tools will follow, before a more systematic and collaborative approach focusing on cybercrime prevention policies is proposed.