Attributing Cyber-Attacks under International Law: A User-Friendly Guide to Busting Unfriendly Ghosts in the Machine

Various malicious activities in cyberspace ostensibly violate international legal rules, universally binding and applicable. By launching such cyber-attacks, assisting other States or allowing non-State actors to do so, States commit internationally wrongful acts, for which they bare legal responsibility. However, in order to establish that a certain State is responsible for a specific cyber-attack, the relevant conduct must be attributed to that State; only then, for instance, the aggrieved State could lawfully retaliate by breaching its own international obligations. The available legal framework therefore lays out diverse grounds for attributing wrongful acts to States, with distinct, substantive requirements for each. Yet this framework says very little on how to make the necessary determinations for substantiating the respective grounds in concrete cases, so that practical questions of attribution abound and mostly remain unresolved. The same issues invariably arise in attempting to attribute cyber-attacks under said framework, which is widely considered to cover States' online conduct and relations, though it formally concerns offline activities alone. Indeed, as in other areas of international law, deploying the rules of attribution to cyberspace not only exacerbates preexisting difficulties in different respects, but also introduces novel challenges, due to the unique qualities of this operational environment. Nevertheless, the technological revolution underlying these vital yet vexing properties, additionally appears to offer new ways for overcoming age-old hurdles to holding States accountable for harmful and unlawful activities.

This presentation aims to provide analytic guidance on the practicalities of attributing cyber-attacks, useful for lawyers and non-lawyers alike. It will firstly map the principal matters and manners of assigning State responsibility for internationally wrongful acts, focusing on the requisite factual findings in the main and ubiquitous scenarios, as well as on the common and unsettled legal aspects of ascertaining such facts. As part of this, we juxtapose malicious cyber-activities to similar and familiar sorts of offline operations, and technological to traditional means of inquiry into either sphere of conduct and relations, in order to distinguish between enduring and emergent problems of attribution. Further, the presentation will briefly touch on the topic's institutional dimension: by drawing both on examples for inter-State fact-finding processes and on the recent flurry of cyber-specific proposals, we distill key structural and functional considerations for designing effective mechanisms for attributing cyber-attacks (while pondering whether that is politically feasible). Finally, the presentation will call for collaborative engagement – by scientists and techies, legal scholars and practitioners, policymakers and experts – in pursuing robust and regular accountability in cyberspace. We thus identify fundamental queries an integrative approach to attribution should address; time permitting, we also proffer possible

answers in this respect, by outlining an original idea for a global and non-governmental array of cyber-guardians.