CPH Definition of DNS Abuse

DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse. The Internet and Jurisdiction Policy Network’s Operational Approaches, Norms, Criteria, Mechanisms provides the following definitions for each of these activities:

- **Malware** is malicious software, installed on a device without the user’s consent, which disrupts the device’s operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.

- **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.

- **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or ‘look-alike’ emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.

- **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to [the attacker’s] site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false IP address bearing malicious code. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.

- **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content. While Spam alone is not DNS Abuse, we include it in the five key forms of DNS Abuse when it is used as a delivery mechanism for the other four forms of DNS Abuse. In other words, generic unsolicited e-mail alone does not constitute DNS Abuse, but it would constitute DNS Abuse if that e-mail is part of a phishing scheme.