ICANN'72 POLICY FORUM, *OCTOBER* 2021

DNS + WEB CONTENT ABUSE: DISINFORMATION

DNS ABUSE: INTRODUCTION

- The Domain Name System (DNS) serves as a crucial system connecting its users and devices to the Internet
  - Prone to abuse

- ICANN GAC statement on DNS Abuse 2020:

  - "If the public is to trust and rely upon the Internet for communications and transactions, those tasked with adminstering the DNS infastructure must take steps to ensure that this public resources is safe and secure"

Before DNS Abuse can be properly addressed, registrars and registries need to have a shared understanding as how to define it

Categories of Abuse – The Framework

- Five key forms of DNS abuse according to the Internet and Jurisdiction Policy Network's DNS abuse Framework
  - Malware
  - Botnets
  - Phishing
  - Pharming
  - Spam
- DNS vs Content Abuse
  - In order to protect freedom of speech, registries and registrars are usually not required to act on web content abuse
  - However, the framework presents cases where registries and registrars must act on content abuse
    - Child sexual abuse materials
    - Illegal Distribution online of opioids
    - Human Trafficking
    - Specific and Credible incitements to violence

WEB CONTENT ABUSE: BOTNETS

- Data-processing algorithms are increasingly influential instruments of perception

- Political bots (most common) are manipulating public opinion over major social networking applications

- Botnets ability to steer the construction of public problems has a direct impact upon the ordering of social and political realities

- "Computational Propaganda" and bots are more likely to appear during or after a crisis - distorting it and creating more damage

- Moments of crisis generate collective uncertainty: audiences highly "influenceable"

CASE STUDY: MANCHESTER BOMBING

British Journal of Sociology Study

- After the bombing, a woman's social media accounts had claimed she was housing over 60 lost children while publicly issuing her phone number through posts on Twitter and Facebook

- Labeled as the 'Angel of Manchester' by the Daily Mail - but the event never occured

- The woman claimed to have nothing to do with the posts or issuing her phone number

- 28 separate similar "Ghost" incidents occurred the same night- adding to the chaos of the bombing

CASE STUDY: BOTNETS & EVENT GHOSTING

FACEBOOK POST:
"DO NOT COME OLDHAM HOSPITAL IM CURRENTLY LOCKED INSIDE... MAN OUTSIDE WITH GUN"

- Post was made moments after the bombing, screengrabbed and retweeted by at least 368 Twitter accounts

- Hospital denied this rumor yet it continued to circulate during aftermath of terror attack

- Ambulances and fire crews stayed behind in order to cater to these 'Ghost Events'

- This episode demonstrates how disinformation communication on social media can have tangible effects on our reality - impede quick action and clear communication

Conclusions & Solutions

- Website content abuses that pose an irreversible threat to human life and civil safety should be discussed for policy in the future

- Incentivize the adoption of proactive anti-abuse measures in Registry Agreement provisions

Questions
Comments
Concerns?