The relationship between crowdsourcing digital activism and cybersecurity

Cassie Lowery, Cohort 3 - cl2491@bath.ac.uk
Dr Laura Smith
Dr Matthew Edwards

Background

Crowdsourced

- Calling on others to contribute to an action
- Must exist outside existing organisational hierarchies

Digital

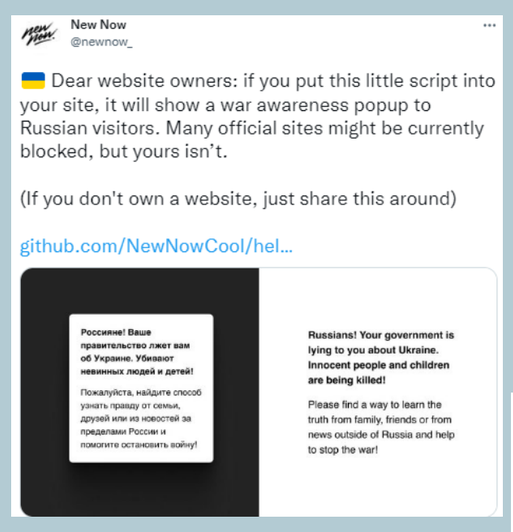
- The action is technologically facilitated

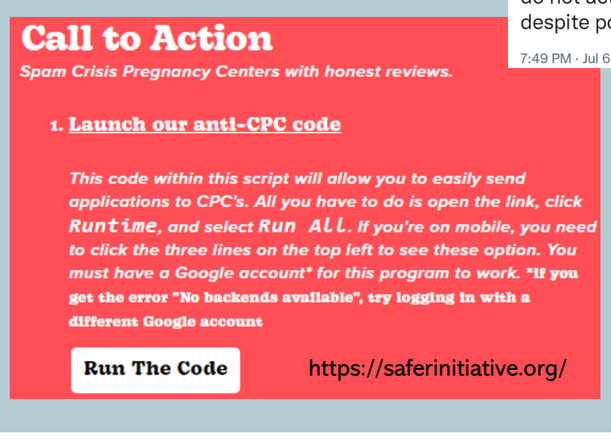
Activism

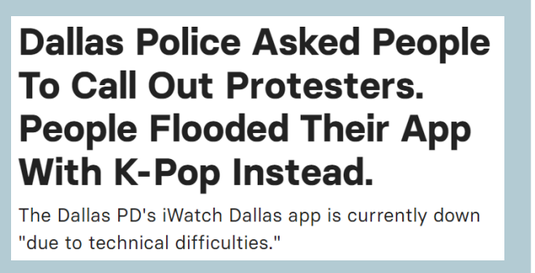
- The action is taken on behalf of an ingroup, i.e., it is *collective* action

Already activists have taken advantage of a wide range of existing technologies, from posting photos on Google reviews, to utilising simple technological tools.

We are seeing a real diversity of tactics and actors, everyone from cybercriminals and hacktivists, to IT professionals, and everyday people.







The problem

Despite how common this type of action seems to be, research is falling behind.

In computer science literature, inconsistent & ambiguous threat topologies make determining when existing categories no longer capture emerging threats difficult, and consequently limit our ability to predict and counter actions

Similarly, in psychology, collective action researchers tend to operate with implicit assumptions that offline actions are more impactful than actions taken online and ignore the impact online actions have on security.

Research Objective:

To understand crowdsourced digital actions and the relationship between technology, users and societal context

Research Questions:

How do technological affordances of platforms and tools used by these groups help them organise and launch attacks?

What are the psychological motivations for taking these actions?

What security threats do they pose, now and in the future?

Next Steps

Taking an interdisciplinary approach, using psychology and computer science as reflected in supervisory team. Applying psychological theories of collective action can help elucidate what forms these attacks take, and why and when they occur. Such work can thus better inform cybersecurity research on threat actors and attack vectors and how these may evolve.

Proposed Methodology

Creation of Database

- Used OSINT search to create database of 31 forms of CDA

Repertory Grid Technique

- Activists Interviews (N = 20) to elicit dimensions underlying actions
- Online survey & cluster analysis inform dimensional typology of CDA

Mixed Methods Analysis & Model Development

- Thematic analysis of posts and websites of group Gen Z for Change, exploring psychological motivations for engaging in different forms of CDA
- Findings to inform codebook used to develop a model for threat detection

Experiments

- Experimental studies testing how manipulating the justifications used affects perceptions of acceptability and willingness to take part

Challenges

Responsible Innovation challenges: need to ensure any proposed countermeasures are not abused and deployed by bad actors and consider how any proposed innovations are instead used to shape desirable futures.

Conceptual challenges: Activist or adversary, and how to draw a distinction