**describe the research questions**

How do repressive nation-states monitor telecommunications for political dissent? Particularly for Bahrain, Syria & UAE?

What are the consequences of opposing the government through technology?

What effect does this have on the given repressive nation-states society at large?

**Contributions**

Understanding of how governments monitor and repress. Known social consequences of opposition.

Understanding of different technologies used including IP spy campaign, RATs, and Remote Control Systems

Gained information can be used as a launching pad for protective security technologies in favor of those being repressed

**methods**

Analyzed an extensive collection of suspicious files and links targeting activists, opposition members, and non-governmental organizations (Noteworthy: Reached out to these groups.)

Sought understanding of government specific monitoring technologies – extensive diagrams on the complications of how the systems function

**results**

Identified commercial spyware marketed exclusively to governments (Gamma’s FinSpy and Hacking Team’s Remote Control System (RCS))

Greater social understanding of consequences for those in opposition of governmental powers (Families lives put in danger for opposition, police admitting to having spied on civilian’s laptops)

**Limitations**

Work began when individuals concerned that a government might have targeted them for cyberattacks – this is very clearly a voluntary action that can only have been taken by individuals who felt that they COULD put themselves at risk, especially considering the social consequences. Researchers proceeded to contact at-risk groups individually with the gained knowledge from the first group. Here, there is very much a clear voluntary admittance of communication. Because this is voluntary, the data that was given may be skewed and biased. It may even be intentionally misleading (if it were a planned government execution).