Watchful Eyes and Silent Voices: Assessing the Transnational Effects of Surveillance on Media Freedom

Students: Aaron Aytes, Yessica Bello-Luna, Lauren Caruso **Mentors: Kathleen Brickner and Dr. Jennifer Henrichsen**

INTRODUCTION

- Personal and media freedom have become much more difficult to sustain. Modern technology allows for surveillance of massive populations. governments, particularly authoritarian governments, have employed the use of extensive camera networks, online networks, and online activity.
- Authoritarian governments employs systematic monitoring of individuals' activities while controlling and manipulating the population. The most prominent countries to employ mass surveillance are also authoritarian regimes, this includes China, Iran, Syria, and Vietnam.
- Extreme surveillance impacts media freedom, the act of monitoring and use of filters allow for the targeting of criticism and identifying individuals who speak out against a regime.
- Mass monitoring would not be possible without the aid of private corporations, which are largely based in democratic nations. These companies sell surveillance equipment and spyware to authoritarian regimes.

EFFECTS OF SURVEILLANCE TECHNOLOGY

- One a transnational scale, surveillance technology is used to:
  - Control information
  - Monitor speech
  - Suppress media freedom
  - Suppress political dissonance
  - Censorship

Figure 1: Graphic depicting examples of Video Surveillance

TYPES OF SURVEILLANCE/SPYWARE

- **Audio Surveillance -** Record and transmit audio. Example: Speaker Identification software which compares recordings against target voice samples.
- **Video Surveillance -** Use video cameras. Example: Wide area persistent surveillance.
- **Location Monitoring:** Monitor the location of a target using phone identifiers or tracking devices. Example: GPS tracking devices.
- **Biometrics -** Identify individuals on distinctive physiological or behavioral characteristics. Example: Facial recognition software
- **Forensics -** When attached to a device, extract and visualize data from it. Example: Commercial software packages offered by surveillance companies.

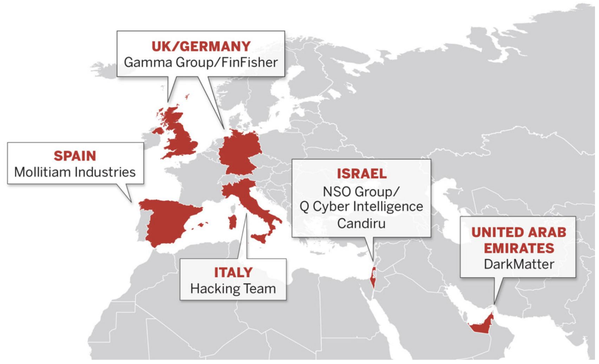

Figure 2: Graphic depicting where some of the most prominent spyware companies are based.

MANUFACTURERS FROM DEMOCRACIES AND LOCATION OF DEPLOYMENT

- **HackingTeam™ -** One of the first companies to develop and sell spyware to governments. Sold and rebranded as Memento Labs™.
  - Evidence the government of Azerbaijan has used HackingTeam™ surveillance equipment's to spy on citizens since 2009. (2009-2013)
  - Leaked documents have exposed Ecuadorian government of illegal spying on politicians, journalists, and activists with HackingTeam™ spyware (2013-2018)
- **Gamma Group/FinFisher™ -** Accused of illegally selling surveillance software to authoritarian governments for years. Filed for insolvency in March 2022, has ceased operations. Accused crimes include:
  - Jordan employed malware to spy on journalists, human rights defenders, and opposition (2015)
- **NSO Group Technologies® -** Israeli based cyber-intelligence firm. Known for its proprietary spyware Pegasus, which is capable of remote zero-click surveillance of smart phones.
  - Egyptian government exposed for using Pegasus spyware to hack dissident phones (2021).
  - Morocco employed spyware targeted civil society & French government officials (2017-2022)

POSSIBLE REGULATORY & LEGAL ACTION TO MITIGATE SPYWARE'S HARM

- **'Know your Customer' framework:**
  - Focused on the review of several different government and company regulations, including what the purchasing of government and company agents say about technologies, before & after sale.
  - Technology needs to be reviewed for its capabilities of violating human rights. Mitigation efforts need to be introduced at this stage.
  - Purchasing government's regulations, laws, and practices regarding surveillance equipment must be vetted before sale.

REFERENCES

A. Aytes, K. Brickner, Y. Bella-Luna, and L. Caruso, "Watchful Eyes and Silent Voices: Assessing the Transnational Effects of Surveillance on Media Freedom," in *IEEE Access*, vol. 7, pp. 108304-108315, 2019, doi: 10.1109/ACCESS.2019.2933415.

ACKNOWLEDGMENTS

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

WASHINGTON STATE UNIVERSITY