Online Behaviour of States
Jaymie Caplen, Gerry Stoker, Tim Chown
Cyber Security Centre
University of Southampton

The Effect of Different Strategies on Populations and International Relations

Overview of Research
There are few states in the world that do not in some way prescribe what online behaviour they consider unacceptable, and the majority intervene to some degree in the day-to-day online lives of their citizens. This is usually through enacting legal provisions, implementing technical measures, or a combination of both. When domestic crises occur, as was seen in the ‘Arab Spring’ of 2010/2011, states will often impose extraordinary measures in an attempt to retain control of a situation or to restore order. This research project aims to establish why differences in approach exist, and to develop a tool that will provide insights into how different intervention strategies will affect both the domestic population of a country and its international relations.

Example of Methodology in Action
The proposed methodology has several distinct stages designed to highlight connections between regime type and intervention policies as well as intervention policy and domestic and/or international reaction.

Stage 0: Selection of Countries to Study
- Authoritarian Regimes
- Totalitarian Regimes
- Democratic Regimes

Stage 1: Review of Day-to Day Situation
- Legal provisions (Internet Monitoring and Filtering)
- Technical capability (Internet Monitoring and Filtering)
- Internet infrastructure (Centralised/Disparate, Gov/Commercially Controlled)

Stage 2: Comparative Analysis
- Explore connections between regime type and day-to-day situation

Stage 3a: Review of Regime Online Intervention Strategies
- Widespread Blocking/Content Filtering
- Online media Hacking/Manipulation/Author Punishment
- Disruption of Mobile Communication Systems
- Internet Blackout

Stage 3b: Collection of Domestic and International Opinion/Reactions to Intervention Strategies
- Opinion directly received through online survey sites
- Analysis of blogs/social media (including Facebook, Twitter and Google+)
- International news reports/editors
- Explicit statements by government officials

Stage 4: Production of Analysis Tool Enabling Prediction of Reaction to Various Online Intervention Strategies
- Exploitation path in Government and Industry (Communication Strategies & Threat Indicators)

Results to Date
A limited version of the methodology (stages 1-3) has been applied to explore intervention approaches adopted by the Tunisian and Egyptian regimes during the ‘Arab Spring’.

Stage 1/2
- Significant technical capability to monitor and filter internet traffic.
- Numerous legal provisions providing for censoring/filtering of content deemed obscene or threatening to public order.
- Online media channels closely monitored; online dissidents’ reactions severe punishments.
- Centralised Internet infrastructure (wholly Gov't-owned).

Stage 2
- Very limited technical capability to monitor and filter internet traffic.
- No legal provisions providing for censoring/filtering of content deemed obscene or threatening to public order.
- Online media channels closely monitored; online dissidents’ reactions severe punishments.
- Disparate Internet infrastructure (mostly commercially owned).

Stage 3
- Notable increase in the blocking of websites (mostly political) using existing technical measures.
- Hacking of social media websites, disrupting & manipulating online accounts.
- Widespread distribution of malware to attack computers & hamper organisation and dissemination of information.
- Large number of online activities identified and targeted.

Stage 3
- All major social networking websites targeted by instructing individual ISPs to block access.
- Limited manual monitoring of social media websites by government officials.
- Internet ‘blackout’ put in place, most likely by instructing individual ISPs to withdraw BGP routes.
- Mobile communications disrupted at the peak of the unrest.

Initial Conclusions from Analysis
1. No clear link between regime type and day-to-day intervention policies in this case; technical infrastructure and expertise more deterministic.
2. Clear link between day-to-day online intervention policies and steps taken during a crisis; technical interventions increased if available, ‘total shutdown’ enacted if not.
3. Outcome of events in Tunisia (collapse of regime and role played by Internet and related technologies) were a key factor in Egyptian government’s formulation of an online intervention strategy.