**Cyber-Influence Operation Analysis:**

**Background, Documentation, and Modelling of Cyber and Disinformation Components.**

# Al-Toufan 2022 defacement of Bahraini and Israeli websites

## Summary

In mid-February, cyber persona Al-Toufan ("the flood" in Arabic) claimed to deface several Bahraini and Israeli websites in conjunction with the 12th anniversary of the outbreak of nationwide antigovernment protests in Bahrain. Al-Toufan used these attacks to fan protests among the politically underrepresented Shi'ite majority in Bahrain by calling attention to poverty and inflation in the region. The group replaced legitimate content on news and government websites with articles that criticized the regime. Replacing the headlines with incendiary comments on the royal family and normalization with Israel and changed articles’ images to photos of opposition figures.

Following the defacement, a fictitious cyber persona publicises and exaggerates the attacks on social media, before sockpuppet Arabic-language social media accounts were later used to amplify the defacements.

## Timeline and Context

Februrary 2022

* Following a successful cyberattack, Bahraini and Israeli pro-government news websites were defaced.
* The Bahrain Airport website was also targeted. The website returned 504 and 404 errors, rendering the services unavailable for at least half an hour in the middle of the day.
* Al-Toufan performed a DDoS attacks on the Bahrain News Agency website and the Bahrain Chamber of Commerce website. Research is inconclusive as to the effectiveness of this attack.
* Al-Toufan uses its presence on social media platforms such as Instagram, YouTube, Twitter, and Telegram to begin publicising and exagerrating the attacks on social media.
  + Al-Toufan announced via Twitter that it had also changed the main page of hundreds of Israeli websites and wrote: "We are in Israel, the war with you will not be only in Bahrain.
  + The group posted propaganda videos with political chants and a collage of exiled or jailed political figures from the opposition (e.g., Ali Salman, Abduljalil AlSingace, Hassan Mushaima, and others) next to the Pearl Monument in Qatar.
* Sockpuppet accounts are used to amplify the exaggerated news.
  + Accounts target messaging towards specific audiences, using the language of the target audience as well as attempting to establish credibility through the impersonation of accounts of a targeted organisation, or a senior official at that organisation.

Defacement and DDoS attacks result in lost revenue, reputational damage, misinformation campaigns, and promotion of Al-Toufan’s agendas. Defacements could cast doubt on the security and legitimacy of the websites’ information.

## Frameworks

### ATT&CK Framework

* TA0043 Reconnaissance
  + T1595 Active Scanning
    - T1595.002 Vulnerability Scanning
* TA0040 Impact
  + T1491 Defacement
    - T1491.002 External Defacement

ONE OF:

* + T1499 Endpoint Denial of Service
  + T1498 Network Denial of Service
    - We know a DoS attack has occurred, but the method is unclear. These remain speculative.

### DISARM Framework

* **PLAN**
  + TA01 Plan Strategy
    - T0073 Determine Target Audiences
    - T0074 Determine Strategic Ends
  + TA02 Plan Objectives
    - T0066 Degrade Adversary
    - T0075 Dismiss
      * T0075.001 Discredit Credible Sources
    - T0076 Distort
    - T0079 Divide
  + TA13 Target Audience Analysis
    - T0072 Segment Audiences
      * T0072.005 Political Segmentation
    - T0080 Map Target Audience Information Environment
      * T0080.005 Assess Degree/Type of Media Access
    - T0081 Identify Social and Technical Vulnerabilities
      * T0081.006 Identify Wedge Issues
* **PREPARE**
  + TA14 Develop Narratives
    - T0068 Respond to Breaking News Event or Active Crisis
    - T0083 Integrate Target Audience Vulnerabilities into Narrative
  + TA06 Develop Content
    - T0023 Distort facts
      * T0023.001 Reframe Context
    - T0085 Develop Text-based Content
      * T0085.003 Develop Inauthentic News Articles
  + TA15 Establish Social Assets
    - T0090 Create Inauthentic Accounts
      * T0090.001 Create Anonymous Accounts
      * T0090.004 Create Sockpuppet Accounts
  + TA16 Establish Legitimacy
    - T0097 Create personas
  + TA05 Microtarget
    - T0101 Create Localized Content
  + TA07 Select Channels and Affordances
    - T0104 Social Networks
      * T0104.001 Mainstream Social Networks
    - T0105 Media Sharing Networks
      * T0105.001 Photo Sharing
      * T0105.002 Video Sharing
* **EXECUTE**
  + TA09 Deliver Content
    - T0115 Post Content
  + TA17 Maximize Exposure
    - T0118 Amplify Existing Narrative
  + TA10 Drive Offline Activity
    - T0126 Encourage Attendance at Events
      * T0126.001 Call to action to attend
  + TA11 Persist in the Information Environment
    - T0060 Continue to Amplify
  + TA12 Assess Effectiveness
    - T0132 Measure Performance
      * T0132.002 Content Focused
    - T0133 Measure Effectiveness
      * T0133.001 Behaviour Changes
      * T0133.002 Content
      * T0133.005 Action/Attitude
    - T0134 Measure Effectiveness Indicators (or KPIs)
      * T0134.001 Message Reach
      * T0134.002 Social Media Engagement

## Resources

https://cyble.com/blog/altoufan-team-targets-the-middle-east/

https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/

https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf

http://bahrainmirror.com/en/news/62313.html

https://apnews.com/article/technology-persian-gulf-tensions-bahrain-9bd1288487bac78362fe4dca0c19a7f4

https://blog.sekoia.io/iran-cyber-threat-overview/

https://www.darkreading.com/cybersecurity-operations/iran-and-the-rise-of-cyber-enabled-influence-operations-

https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-296b