**Cyber-Influence Operation Analysis:**

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

# Anonymous Sudan – Involvement in Israel-Hamas Conflict

## Summary

On the 7th of October 2023, a group operating under the name “Anonymous Sudan” launched several DDoS attacks on Israeli websites. These websites included the Jerusalem Post, Israeli Security Agency (Mossad), and Prime Minister’s website. Due to the DDoS attacks, the websites were temporarily made unavailable. Anonymous Sudan has multiple telegram channels where they displayed these attacks. The group also took responsibility for an attack on Israeli warning systems, which alert citizens of potential danger. On the same day (the day of an attack by Hamas against Israel), DDoS attacks were launched against two companies that provide online alert systems. According to one of the companies, Red Alert, only the website was affected, and the alert system was still able to send alerts to users. Anonymous Sudan also targeted Australian education websites, a Jewish hospital in LA and a series of American companies, in retaliation for these organisations supporting Israel or demonstrating values antithetical to Pan-Islamism.

## Timeline and Context

**October 7th, 2023**

* Anonymous Sudan launched > 40 DDoS attacks on Israeli websites
  + These sites include the Jerusalem Post, Israeli Security Agency (Mossad), and Prime Minister’s website.
  + The websites were made temporarily unavailable, significantly affecting the Jerusalem Post in particular.
  + The DDoS attacks were achieved using Anonymous Sudan’s DDoS tool, a botnet / distributed cloud attack tool.
* Anonymous Sudan also launched DDoS attacks on Israeli alert systems
  + They used DDoS attacks against two companies that provide online alert systems, which alert Israeli users of incoming danger.
  + This occurred approximately an hour after Hamas began their attack.
  + According to the New York Times, the systems were briefly disabled. However, the company Red Alert stated that their alert system was unaffected, and only their website was offline.
* The group has multiple channels on Telegram, an encrypted chat app, with over 80,000 followers.
  + As the attacks took place, Anonymous Sudan updated their telegram channel with messages related to their attacks. Messages included:
    - “We are currently targeting some critical endpoints in the alert systems of Israel”
    - “Glory to the Palestinian Resistance, we are with you.”
    - “Infrastructure of the Israeli has been down because of what they did to Palestine”
  + They also use their channels to advertise their DDoS services for hire. They use Bitcoin to make transactions with customers.
  + From their activity on telegram, their motivation is both financial and ideological. They support Hamas and promote the group’s ideals.

**General activity**

* Additionally, Anonymous Sudan launched DDoS attacks on several American companies, Australian Education Institutions, and many hospitals.
  + The group targets organisations that support Israel or that demonstrate non-Muslim values.

## Frameworks

Description and Justification of the techniques can be found in the corresponding intermediary table document.

### ATT&CK Framework

* **TA0043: Reconnaissance** 
  + T1593.002: Search Open Websites/Domains: Search Engines
  + T1590.00: Gather Victim Network Information: Domain Properties
  + T1593.001: Search Open Websites/Domains: Social Media
  + T1594: Search Victim-Owned Websites
* **TA0042: Resource Development**
  + T1588.002: Obtain Capabilities: Tool
  + T1583.004: Acquire Infrastructure: Server
  + T1583.005: Acquire Infrastructure: Botnet
* **TA0040: Impact**
  + T1498: Network Denial of Service
  + T1489: Service Stop

### DISARM Framework

* **PLAN**:
  + TA01: Plan Strategy
    - T0073: Determine Target Audiences
    - T0074: Determine Strategic Ends
  + TA02: Plan Objectives
    - T0066: Degrade Adversary
    - T0078: Dismay
    - T0075: Dismiss
  + TA13: Target Audience Analysis
* **PREPARE**:
  + TA14: Develop Narratives
    - T0068: Respond to Breaking News Event or Active Crisis
  + TA15: Establish Social Assets
    - T0093.002: Acquire Botnets
    - T0090.001: Create Anonymous Accounts
    - T0092.003: Create Community or Sub-group
  + TA06: Develop content
    - T0085: Develop Text-Based Content
  + TA07: Select Channels and Affordances
    - T0043.001: Use Encrypted Chat Apps
    - T0043: Chat Apps
* **EXECUTE**:
  + TA09: Deliver Content
    - T0115: Post Content
  + TA11: Persist in the Information Environment
    - T0128.001: Use Pseudonyms
    - T0128.002: Conceal Network Identity
    - T0130.004: Use Cryptocurrency
    - T0060: Continue to Amplify
  + TA18: Drive Online Harms
    - T0123.002: Block Content
    - T0123: Control Information Environment through Offensive Cyberspace Operations
    - T0048: Harass
* **ASSESS**
  + TA12: Assess Effectiveness
    - T0134.001: Measure Effectiveness Indicators (or KPIs): Message reach

## Resources

This includes resources used to produce a timeline, technical information, tactics, techniques, and procedures used in the operation. It can also include any relevant resources that support modelling decisions such as technical methods for cyber components or societal/psychological context for influence components.

<https://cybernews.com/news/anonymous-sudan-targets-israel-mossad-netanyahu/>

[https://blog.cloudflare.com/ddos-attacks-on-australian-universities/?\_gl=1\*7ad1re\*\_gcl\_au\*NzEyMzY5MDQ5LjE3Mjk0ODMyOTA.\*\_ga\*NTU5NjQ0NDU1LjE3Mjk0ODMzMjE.\*\_ga\_SQCRB0TXZW\*MTcyOTQ4MzMyMC4xLjEuMTcyOTQ4MzQyNS42MC4wLjA./](https://blog.cloudflare.com/ddos-attacks-on-australian-universities/?_gl=1*7ad1re*_gcl_au*NzEyMzY5MDQ5LjE3Mjk0ODMyOTA.*_ga*NTU5NjQ0NDU1LjE3Mjk0ODMzMjE.*_ga_SQCRB0TXZW*MTcyOTQ4MzMyMC4xLjEuMTcyOTQ4MzQyNS42MC4wLjA./)

[https://blog.cloudflare.com/ddos-attacks-on-australian-universities/?\_gl=1\*7ad1re\*\_gcl\_au\*NzEyMzY5MDQ5LjE3Mjk0ODMyOTA.\*\_ga\*NTU5NjQ0NDU1LjE3Mjk0ODMzMjE.\*\_ga\_SQCRB0TXZW\*MTcyOTQ4MzMyMC4xLjEuMTcyOTQ4MzQyNS42MC4wLjA./](https://blog.cloudflare.com/ddos-attacks-on-australian-universities/?_gl=1*7ad1re*_gcl_au*NzEyMzY5MDQ5LjE3Mjk0ODMyOTA.*_ga*NTU5NjQ0NDU1LjE3Mjk0ODMzMjE.*_ga_SQCRB0TXZW*MTcyOTQ4MzMyMC4xLjEuMTcyOTQ4MzQyNS42MC4wLjA./)

<https://www.cloudflare.com/en-gb/learning/ddos/glossary/anonymous-sudan/>

<https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals>

<https://www.washingtonpost.com/technology/2024/10/16/sudanese-charged-cyberattack-gang/>

<https://www.washingtonpost.com/technology/2023/10/09/cyber-attacks-gaza-hamas/>

<https://www.jpost.com/international/article-825144>

<https://www.jpost.com/israel-news/article-741869>

<https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals>

<https://www.justice.gov/usao-cdca/media/1373586/dl?inline>

<https://www.justice.gov/usao-cdca/media/1373581/dl?inline>

<https://www.wired.com/story/israel-hamas-war-hacktivism/>

<https://time.com/6322175/israel-hamas-cyberattacks-hackers/>

<https://cybercx.com.au/blog/hamas-israel-conflict/>

<https://www.nytimes.com/2024/10/18/world/middleeast/anonymous-sudan-cyberattack-indictment.html>

<https://www.cloudflare.com/en-gb/learning/ddos/glossary/anonymous-sudan/>

<https://cybernews.com/news/anonymous-sudan-targets-israel-mossad-netanyahu/>

[https://blog.cloudflare.com/ddos-attacks-on-australian-universities/?\_gl=1\*7ad1re\*\_gcl\_au\*NzEyMzY5MDQ5LjE3Mjk0ODMyOTA.\*\_ga\*NTU5NjQ0NDU1LjE3Mjk0ODMzMjE.\*\_ga\_SQCRB0TXZW\*MTcyOTQ4MzMyMC4xLjEuMTcyOTQ4MzQyNS42MC4wLjA./](https://blog.cloudflare.com/ddos-attacks-on-australian-universities/?_gl=1*7ad1re*_gcl_au*NzEyMzY5MDQ5LjE3Mjk0ODMyOTA.*_ga*NTU5NjQ0NDU1LjE3Mjk0ODMzMjE.*_ga_SQCRB0TXZW*MTcyOTQ4MzMyMC4xLjEuMTcyOTQ4MzQyNS42MC4wLjA./)

<https://archive.md/1lJIL#selection-4991.0-4991.17>

<https://cybernews.com/cyber-war/pro-russian-hacktivists-swarm-australian-schools/>