Cyber Crisis Briefing: Legal and Policy Responses to Escalating Conflict

Introduction

Iran has been experiencing anti-government protests since the end of 2025, and at the end of February 2026, a co-ordinated Israeli and US operation struck Iran. This has resulted in polarisation globally.

Hypothetical Scenario:

The conflict continues to escalate, pulling in a number of nations. South Africa has a special treaty with Iran and is therefore placed in an awkward position between providing political support to the Iranian government increasingly under pressure, and trade partners opposing the Iranian government. Consequently, South Africa opts for a middle ground. This upsets the Iranian government, groups internal to South Africa who strongly support the Iranian government, as well as anti-government groups inside of Iran.

As the conflict escalates, so does the cyber dimension. South Africa becomes a victim of a number of cyber incidents:

- A number of government websites are defaced (both pro-Iranian government and anti-Iranian government);
- Distributed Denial of Service attacks targeting the financial sector and diplomatic missions in South African and South African representation abroad;
- Automated disinformation campaigns regarding the South African government's apparent failure to support the Iranian regime;
- Advanced malware found in oil processing facilities.

Three possible sources for these incidents are identified: an emerging internal hacktivist group supporting the Iranian government, Iran-based hacktivists (anti the Iranian government), and an international advanced persistent threat group with ties to the Iranian government.

Tasks and Objectives

Assess the hypothetical scenario and provide a briefing to the national cybersecurity body, based on a policy and legal analysis of the incident. The briefing should be provided in a one-page briefing document and a 3-minute (maximum) presentation (in the form a video) outlining the key points of your briefing document.

Key Tasks

You are an expert group advising South African national cybersecurity decision makers on the recent incidents. You need to prepare a short briefing highlighting the legal and policy options (based in local and international laws and processes) available to counter each of the possible threats (or a combination thereof).

In your 3 minutes video-submission, you are expected to:

- Provide an introduction to the briefing and the situation
- Identify both South African and International laws and policies that could be leveraged to respond to the cyber incidents
- As explanation of how the various laws are relevant to approaching a response to each of the threats
- An estimation of which of the following threat actors presented the most severe risk to South Africa, and the response should be prioritised based on the legal/policy analysis

Your briefing (both the document and video) should be practical and easy to follow, ensuring the cybersecurity decision makers can obtain the information they require quickly.

Final Requirement

April 7th, 12:00PM CET/SAST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

The UKZN is a major public university in South Africa, established in 2004 through the merger of the University of Natal (founded in 1910) and the University of Durban-Westville (established in the 1960s). It is one of the country's leading research-intensive institutions, with a strong reputation for academic excellence and innovation. According to the Centre for World University Rankings UKZN is ranked 4thin South Africa and between 424th -618th globally (dependent upon ranking system) and is considered as a top tier University. UKZN places strong emphasis on research, postgraduate training, and community engagement, making it a hub for both local and international scholars.