



Cyber Diplomacy Workshop  
Addis Ababa, 15th-16th April 2024

# Digital Diplomacy Case Study: Regional Critical Systems Case

© Dr. Katherine W. Getao, 2024

## Case Description

This case is completely fictitious and designed to illustrate features of cyber diplomacy.

It concerns 3 African countries located in the fictitious Mid-East Region (MER) of Africa. Each of the 3 countries has digital ambitions but they are at different stages of development. The case describes a situation where tensions arise in the region due to a series of incidents involving critical systems, critical infrastructure and the digital economy. You do not need strong digital skills to analyse the case; your diplomatic training and experience combined with information shared during this course will be sufficient.

Participants will be divided into groups. Each group should assign a moderator and a rapporteur. Each group shall study and discuss the case and answer the questions posed. Please make a record of the key points noted and the answers to the questions so that the group's contribution may be shared with the wider audience.

Participants have dedicated time to discuss the case in line with the questions provided. A few groups will be selected (randomly) to share their feedback with the meeting as time allows. Participants will have an opportunity to comment on the feedback as they wish.

### Case Study Programme: 15 April, 2024.

<b>Time</b>	<b>Activity</b>	<b>Facilitator</b>
15:30 – 15:40	Case Study introduction, clarifications and group organization	Katherine Getao
15:40 – 16:25	Case Study Analysis in groups	Each group will select a chair and rapporteur. A facilitator from the seminar team may join each group.
16:25 – 16:40	Case Study Reports and questions from the floor (time-permitting)	Randomly selected groups
16:40 – 16:45	Learning and Wrap Up	Katherine Getao

# 1. Background Information

## 1.1 Country Descriptions

### I. Zamunda:

- **Background:**
  - **Zamunda** is a landlocked African nation with limited digital infrastructure.
  - Zamunda relies on its neighbour Mendo for critical connectivity via an optical fibre cable which connects to the rest of the world through the SEAWAYS submarine cable (which is connected to the African Indian Ocean Island of **Danco**.)
- **Situation:**
  - The President of Zamunda aims to launch a **national digital birth registration drive in just 3 weeks time**.
  - The success of this initiative depends on:
    - **Availability of the Fiber Link:** The optical fiber cable connecting Zamunda to Mendo must remain operational.
    - **Data Center Reliability:** A commercial data center in Kiria (Mendo's port town) hosts both the birth registration system and the birth registration database on its cloud infrastructure.
- **Risk Factors:**
  - **Dependency:** Zamunda's entire digital birth registration process relies on Mendo's critical infrastructure.
  - **Security:** Any disruption to the fibre link or data centre could jeopardize the birth registration drive.
- **Scenario:**
  - Zamunda's President sends a diplomatic note to Mendo, emphasizing the criticality of maintaining the fibre link and data centre availability.
  - Meanwhile, the regional Cybersecurity Incident Response Team (MerCIRT) hosted in neighbouring **Bakamoto** has informed officials in both Zamunda and Mendo that an unknown threat actor has been observed to be probing vulnerabilities in the fibre link and data centre infrastructure. MerCIRT is still monitoring the situation.

### II. Mendo:

- **Background:**
  - Mendo is technologically advanced and hosts the critical infrastructure.
  - **Data Center Reliability:** A commercial data centre in Kiria (Mendo's port town) hosts both Zamunda's birth registration system and the birth registration database on its cloud infrastructure. Strict service level contracts and quality of service guarantees have been signed between the Data Center and Zamunda's government to ensure that the systems will work.
  - Mendo's economy thrives on maritime trade and digital services.

- **Role:**
  - Mendo must ensure the uninterrupted operation of the fibre link and data centre.
  - The arrangements that Mendo will make to protect the system in response to Zamunda’s diplomatic note will impact Zamunda’s birth registration drive.
- **Challenges:**
  - **Critical Infrastructure:** Mendo has a single, coastal landing point with only one SEAWAYS submarine cable connecting Mendo to the rest of the world. There is also a single land optical fibre cable route connecting Mendo to Zamunda, from the port of Kiria in Mendo to the border town of Basha in Zamunda.
  - **Data Center Control:** The Government of Mendo has no access rights to the Commercial Data Centre and must rely on the regulator to control its activities through policy and legislation.
  - **Balancing Priorities:** Mendo must safeguard its own interests while supporting Zamunda. Mendo is very conscious of its economic reliance on the perception of being the regional leader in digital services.
  - **Security Measures:** Mendo’s security team must detect and prevent any cyber threats targeting the fiber link and data centre.
- **Response:**
  - Mendo acknowledges Zamunda’s request and initiates security protocols.
  - They collaborate with Zamunda to secure the birth registration infrastructure.
  - They keep abreast of the security reports provided by MerCIRT in Bakamoto, but due to regional rivalry, do not have a close working relationship with the CIRT.

### III. **Bakamoto:**

- **Background:**
  - Bakamoto is a coastal neighbour of both Zamunda and Mendo.
  - Their economy revolves around finance, oil, and tech startups.
- **Role:**
  - Bakamoto, once a digital underdog, now stands at the precipice of offering cutting-edge digital connectivity services. Their coastal town of Abana birthed a project—funded by an Asian benefactor. This fiber-optic marvel stretches from Abana, winding through hills and valleys, until it kisses the border with Zamunda.
  - Bakamoto’s emissaries, have determinedly approached Zamunda. “Our fibre,” they say, “is new, resilient, and eager to serve. Let it be your lifeline to the world.”
  - Bakamoto’s hosts the regional cyber intelligence agency, MerCIRT, and monitors regional threats.

- **Risks:**
  - **State-Sponsored Hackers:** MerCIRT has indicated suspicions that unfriendly nation states may exploit the critical Birth Registration drive to foment regional tensions.
  - **Criminal Groups:** Cybercriminals might seek financial gain or disrupt the birth registration process.
- **Response:**
  - Bakamoto is sharing threat intelligence with Mendo and Zamunda.
  - They offer to provide experts to identify and neutralize the threat, if requested.

The clock is ticking, and the fate of Zamunda’s digital ambitions hangs in the balance. Participants must act swiftly to secure the birth registration infrastructure and thwart any cyberattacks.

## 1.2 Additional Information

### I. Zamunda’s Dilemma:

- **Zamunda**, a landlocked realm, gazes upon the two connectivity suitors: Mendo and Bakamoto.
- Mendo, with its seasoned fibre, has been Zamunda’s trusted companion. Their digital alliance has weathered storms and safely transmitted secrets.
- **Bakamoto**, the newcomer, whispers promises of faster speeds, lower latency, and a direct link to the **SEAWAYS submarine cable**—the global gateway.

### II. Trust and Tension:

- Zamunda hesitates. Trust, like a delicate filament, binds nations. Mendo’s reliability is etched in history, but Bakamoto’s allure is undeniable.
- Diplomats sip tea, their brows furrowed. The Koboros, a secessionist faction in Mendo who repeatedly issue anonymous threats against Mendo’s critical infrastructure, stoke the flames. Their suspected association with Bakamoto raises eyebrows.
- Zamunda’s leaders weigh the scales: tradition versus progress, loyalty versus opportunity.

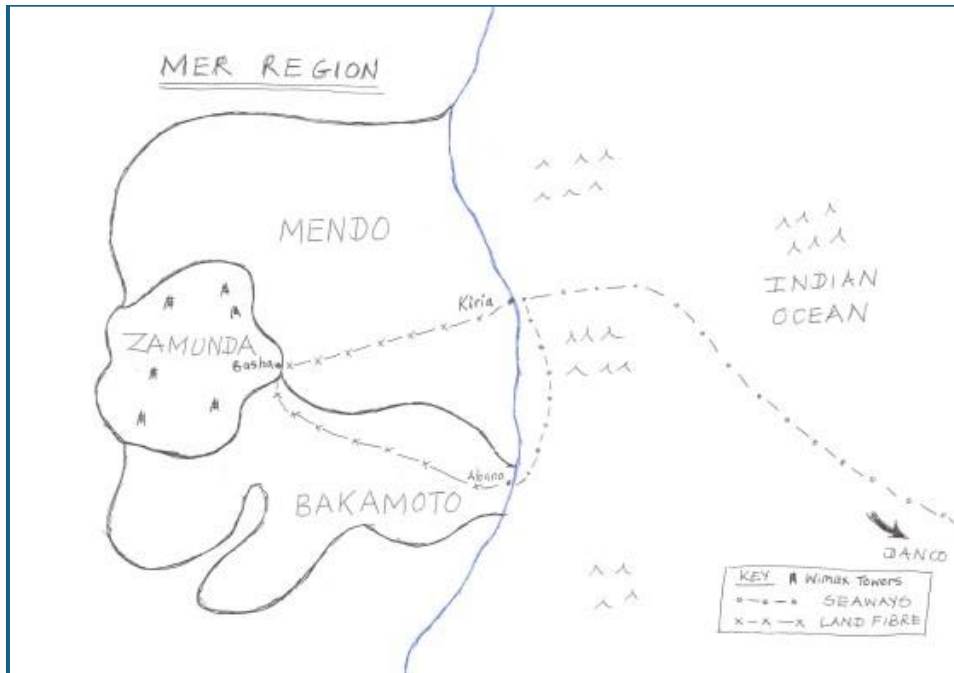
### III. A Lurking Threat:

- **Danco**, the Indian Ocean nation (Africa) where the SEAWAYS cable terminates is well served with optical fibre with 16 Submarine Cables connecting to various Asian nations, Australia and the western coast of the United States of America.
- **A group of researchers at Danco University** in collaboration with researchers from Europe and United States of America have recently published an academic research paper in a respected journal. The paper

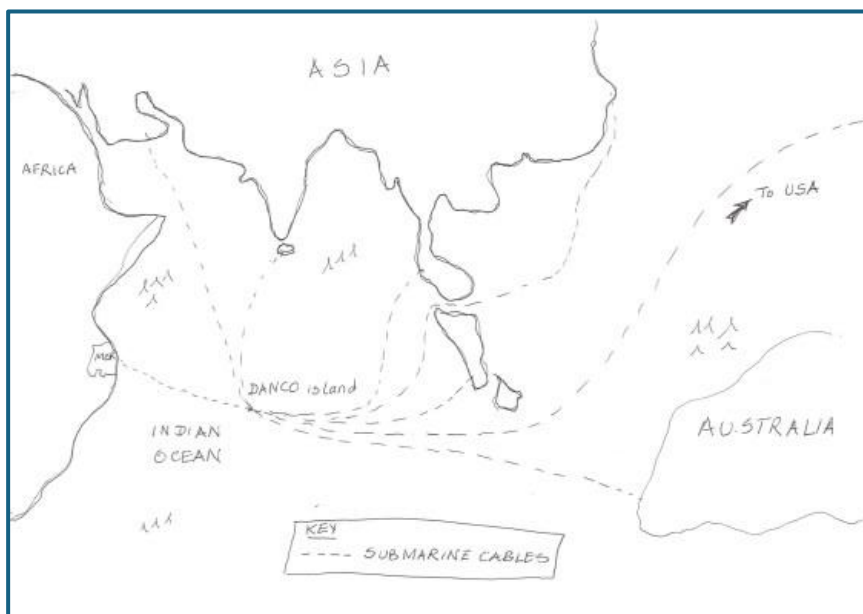
details their research demonstrating that a Quantum Computing Algorithm that they have recently developed can decrypt (remove the code and display in plain text) real time communications passing through optical fibre cables.

- In a demonstration of the efficacy of the new algorithm, an unknown person has recently posted some decrypted sensitive communications on the popular “INTELLEAK” portal (a global website where civil activists, researchers and even (it is claimed) countries post leaked intelligence data.)

Map 1: MER Region



Map 2: Danco Island Submarine Cables



## 2. The Case Scenario

### 2.1 The Stakes:

- The fibre link between Zamunda and Mendo, like a lifeline, must remain unbroken. Registrars need real-time access to the birth registration system.
- The data centre must stand resilient. Any outage could delay the issuance of birth certificates, affecting countless lives in Zamunda and embarrassing the Government.

### 2.2 The Diplomatic Note:

- Zamunda's diplomats have penned a note to their Mendoan counterparts.
- The note reads: "Our birth registration drive approaches. Our schools await the registrars, and our citizens yearn for official recognition. But behold, our reliance on your fibre link and the data centre is absolute. We beseech you: ensure quality of service and availability during this critical time. Remember that the international press watches, poised to amplify any disruption. The eyes of the world rest upon Zamunda."
- The diplomatic note was followed by a personal call from the President of Zamunda to the President of Mendo, emphasizing the same issues.

### 2.3 The Fateful Incidents:

- One week before the birth registration drive, chaos erupts. **Three major fibre cuts**, in swift succession, slice through the Mendo-to-Zamunda link.
- The Koboros secessionist group in Mendo claim responsibility. Their message echoes through the digital ether: "Mendo bleeds. Victory for our just cause transcends borders." The Koboros are a secessionist group in Mendo which have been fighting to create an independent state in the region at the Mendo / Bakamoto border. Members of Koboros largely belong to an ethnic group that spans the border of Bakamoto and Mendo, with the highest population hosted in Bakamoto, although, in Koboros' demands, their new state would carve five times as much land from Mendo than from Bakamoto.
- 6 hours after the third fibre cut, the **commercial data centre in Kiria, Mendo, is hit with a ransomware attack** which locks access to all data stored on their infrastructure. One of the fibre cuts is preventing the data centre from accessing a mirror site which is located in Danco. Subsequently, the **mirror site in Danco** also reports a similar ransomware attack. The group claiming responsibility calls itself **FireFire**, and is demanding 50 million dollars ransom to decrypt the data in the two data centres.
- Panic ripples across Zamunda. Registrars clutch their PDAs, fearing data blackout. The commercial data centre in Kiria, Mendo, trembles, anticipating failure to meet strict service level agreements leading to financial penalties and litigation.

## 2.4 Fanning the Flames:

- A day after the fibre cuts and ransomware attacks, before service has been restored, a damning letter is published on the INTELLEAKS portal.
- INTELLEAKS posts a verbatim decryption of an intercepted sensitive electronic communication from the Government of **Bakamoto** to the **Asian partner** who constructed their newly-completed fibre link.
- The letter reads: “We need your urgent help to connect the Bakamoto fibre to Zamunda so that their priority Birth Registration drive can proceed seamlessly in case of digital failures in our neighbour, Mendo. This is a **golden opportunity** to demonstrate the superiority of Bakamoto’s fibre link!”
- The letter is dated two days before the fibre cut incident in Mendo commenced.
- INTELLEAKS has refused to disclose the source of the leaked communication but many people around the world suspect that it is another demonstration of the power of the Quantum Computing Decryption Algorithm developed by **Danco** researchers in collaboration with others from the Western Hemisphere, and that it was **probably leaked by a Dancoan professor from Danco’s National University**.

## 2.5 Regional Standoffs:

- After the publication of the INTELLEAKS letter the **President of Mendo releases a fiery tweet** to the global X social media platform reading ***“It is clear that my brother in Bakamoto is an enemy of progress. His efforts to destroy the longstanding friendship between Mendo and Zamunda and to destroy Mendo’s digital economy WILL FAIL!!!”***
- The **President of Bakamoto swiftly counters** on the same platform with the **message *“How embarrassing when a country relies on faked communications for their intelligence! It is better to repair that which is broken and restore services to those who need them than to point fingers at an innocent bystander; One who is eager to assist a suffering neighbour who failed to heed advance warnings and mitigate predicted risks!!!”***
- **Zamunda** is also engaged in **desperately seeking help from all well-wishers** in a frantic bid to salvage the rapidly approaching birth registration exercise.



## Exercise for Participants

To reduce tensions in the region, the African Union Commission has invited four countries: Bakamoto, Danco, Mendo and Zamunda to a round table discussion about the digital incident and its resolution.

**You play role of advisor to the AUC, assisting it to understand the open issues and possible ways ahead.**

In this role, your task is to:

- a. Prepare a guide for the meeting with a discussion agenda along three lines:
  - i. Political Issues
  - ii. Diplomatic Issues
  - iii. Digital Issues

Optionally, you may also propose certain policy options to be taken.

- b. Suggest “well-wishers” that Zamunda could approach for assistance (including countries involved in the scenario but also out of it, as well as the private sector, academia, or other stakeholders).