IN ASSOCIATION WITH

MODEL ANSWER B

CAPSTONE: CASE STUDY ESSAY

Assess the likelihood of an Iranian-backed cyber security threat to the water supply in Riyadh, and develop a plan for the Ministry of Interior that

- **responds to this threat by covering prevention, mitigation and response,**
- **utilizes international best practices, and**
- **is consistent with the ethical and legal responsibilities of security officers.**

Riyadh's water supply is uniquely vulnerable to disruption through a concerted, state-back cyber-attack.

A first analytical step is Open Source Intelligence collection. Despite its arid environment, Riyadh uses 3.15 million cubic metres of water a day (Argaam, 2018), with just one day's worth kept in emergency storage tanks (Ratcliffe, V, 2019). Water is provided to Riyadh through two main routes: pipelines from the east coast and local Riyadh-based water storage and treatment plants.

Given the history of Iranian-back cyber-attacks on Saudi assets (4 in the last four years alone) (Baezner, 2019; Paganini, 2020), and the general vulnerability of Middle Eastern countries to cyber-attacks (85% of companies surveyed had fallen victim to an attack – Witt 2020), combined with Riyadh's arid environment, the likelihood of an attack on Riyadh's water supply can be described as a matter of when, not if. If such an attack were to happen it can have serious implications. One of the worst-case scenarios was given by a CSIS (Jones et al.) report, which claimed that an attack on the desalination plant at Jubail would force Riyadh to evacuate "within a week," as the plant provides over 90% of the city's drinking water.

Geographic Information Systems provide an excellent way to analyse the extent of Riyadh's vulnerability, and provide a framework for any response. This can be seen through the following two maps: Figure 1 shows the overlap of population density and water use; Figure 2 shows the location of water treatment plants and their proximity to areas of high water demand.

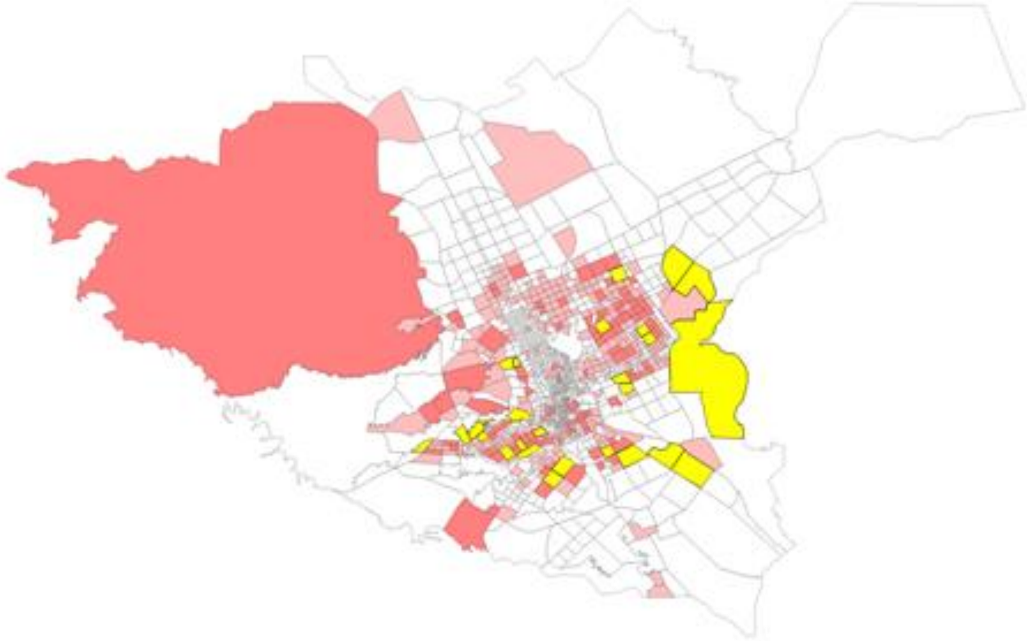

Figure 1: Population and Water Use Density Map (darker red means higher population density; yellow identifies very high water use)

Looking at the risk of an attack on water infrastructure through these maps allows us to differentiate between a macro view – in which attacks are both likely and catastrophic – and a micro view – in which attacks may well be preventable and the results of which may well be more limited.

Figure 1 shows that residential population density is highly variable across Riyadh. In the event of any attack, much of the commercial space can be closed, and water relief efforts can focus on those residential areas that need it most. Figure 2 shows an additional level of localization in water risk: there are six water treatment plants in Riyadh, but just one of them (show by the orange dot) is most closely linked to the high water use area.

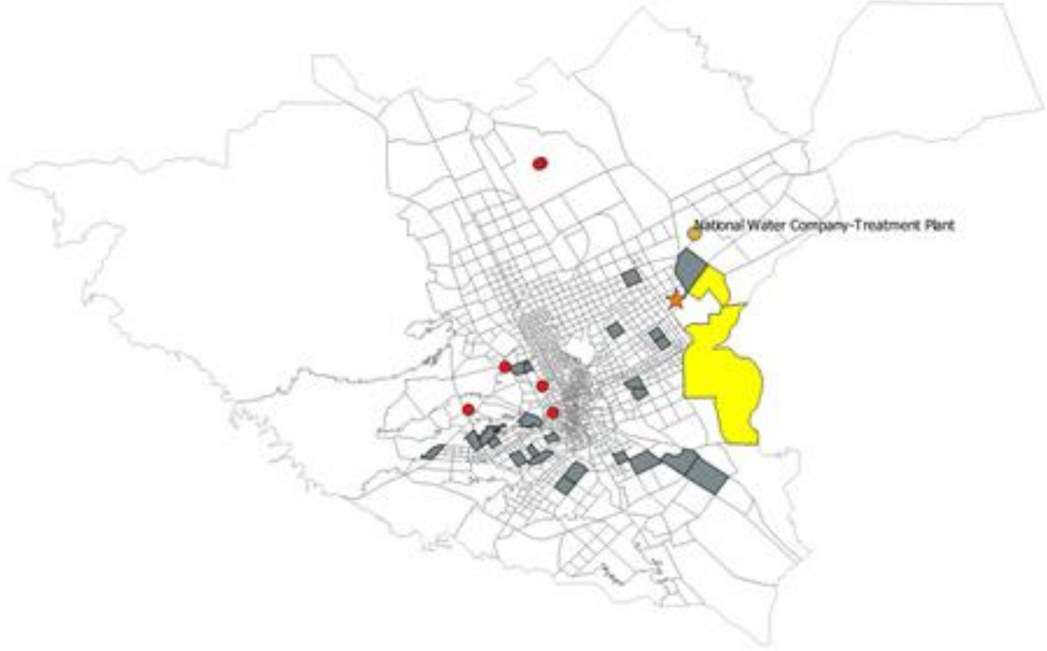

Figure 2: Locations of Water Use (yellow), Population Hotspots (grey), and Water Treatment Plants (red circles)

A constraint in this analysis is that it does not take account of the pipeline network that brings water to Riyadh. However, these pipelines are most vulnerable to physical attacks rather than cyber-attacks and, in the case of any attack on the pipelines, water loss will likely to be total.

Under this scenario, in which there is one high risk treatment plant and one high risk area, the prevention, mitigation and response plans must be tightly focused. Physical and cyber security at the identified water treatment plant should be audited by internationally accepted experts, and their security practices enhanced in response to the findings of this audit as the first step in preventing any major attack. This may include more frequent training in cyber security, enhanced back ground checks on employees and contractors, and a review of all software and IT policies (to purge any malware and ban the use of personal email or USB drives).

There are two considerations here: one legal and one cultural. Any background checks must be compliant with the law, and should not be used to profile or discriminate potential employees for grounds outside those required by law. Second, the training should be adapted to fit the cultural complexities of Saudi Arabia and ownership and implementation of the training program should be transferred to the MOI once it has been developed. Having a company official tasked with responsibility for legal and ethical compliance should help monitor the implementation of screening and training.

In addition, although training programs would increase the security IT should conduct routine checks on their systems to ensure all workers are following proper procedures and employees that are consistently not following proper procedures should be sanctioned by their supervisors.

Mitigation measures can be built around the multiple treatment plants in Riyadh. At the moment, water usage rates are such that there is little spare capacity in the system (Ratcliffe, V, 2019). Capacity additions to each of the current water treatment plants, combined with increased storage capacity (from one day to one week), should mitigate the severity of an attack on an individual plant. It should be noted that such infrastructure investments are highly costly and, because they add only redundancy and spare capacity to the system, will not be profitably under any normal return on investment analysis. Nevertheless, the added capacity will provide a longer buffer in cases of emergency which will give more time for the Ministry to react in cases of emergency thus it is still worth the investment. Higher levels of the Ministry would need to approve this plan and assign funding as well as officers to oversee the project. This plan would increase the capacity, but the new plants would still be vulnerable to a joint attack if they are put on the same software network. To avoid this each plant should have a separate cybersecurity network that is isolated from the rest of the plants.

Response plans must be scalable. At the core they will rely on increased trucking of water into affected areas and widespread water rationing in Riyadh to compensate for the reduced supply. Water storage supplies can be released but must be done in a controlled fashion to ensure they last long enough for repairs to be carried out. This may include the shutting of all water-intensive industry and commercial businesses, the shutting off of domestic water supplies during certain hours, and public information campaign to limit non-essential water use (e.g. car and house cleaning). Water rationing may generate discontent amongst citizens if not properly explained. A clear information campaign and increased police presence at water distribution locations could help control any civil unrest. Of special concern in Saudi Arabia is how families can receive water if the men are away at work during the day. Some families may not be comfortable with women interacting with male water-distribution staff; either female staff, or female-only collection times, should be included in the distribution process. If Riyadh does not have enough water trucks for water distribution extra trucks should be requisitioned from other cities.

The overall plan will be able to ensure the safety and wellbeing of Riyadh's citizens which is our mandate and responsibility as MOI security officers. The strengthened cybersecurity measures will help prevent cyber-attacks from happening in the first place. If those measures prove inadequate in preventing an attack from happening the increase water storage capacity will provide more time for the Ministry to do any necessary repairs, during which time water rationing will be implemented in Riyadh until repairs are complete.

References

- Argaam Special (2018, August 26). *Saudi Arabia consumed 3 bln cubic meters of drinking water in 2017*. Argaam. https://www.argaam.com/en/article/articledetail/id/567200.
- Baezner, M. (2019, May). *Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions*. Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf.
- Jones, S., Harington, N. and Bermudez Jr., J. S. (2019, August 5). *Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.-Iranian Escalation*. Center for Strategic and International Studies. www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation.
- Paganini, P (2020, February 9). *The number of cyber-attacks on Saudi Aramco is increasing*. Security Affairs. https://securityaffairs.co/wordpress/97527/breaking-news/saudi-aramco-under-attack.html.
- Ratcliffe, V. (2019, November 18). Attacks on Aramco Plants Expose Risks to Saudi Water Supply. Bloomberg. https://www.bloomberg.com/news/articles/2019-11-18/attacks-on-aramco-plants-highlight-risk-to-saudi-water-supply.