# MEMORANDUM

**To:** National Security Council
**From:** AU Cyber sQuad
**Subject:** Cyber Attack at the Qatar Ras Abu Fontas Desalination Plant

## Strategic Objectives

- **Investigate** actors and TTPs associated with the backdoor and malware, leveraging diplomatic and intelligence capabilities
- **Mitigate** vulnerabilities in US systems, and offer assistance to improve the resilience of affected countries
- **Communicate** with global partners and the general public to share information, raise awareness of potential threats, and safeguard our systems
- **Anticipate** and minimize emergent technical, policy, humanitarian, and diplomatic risks

## Incident Summary

On November 21, 2022, the first day of the FIFA World Cup hosted in Doha, the Qatar Electricity & Water Co. (QEWC) Ras Abu Fontas desalination plant experienced a cyberattack impacting their temperature control systems. Desalination was disrupted for eleven hours, and full operations resumed approximately four days later. QEWC relied on a version of Yuma software, a common industrial control system (ICS), that was compromised with a backdoor (STANDINGPALM) via a malign software update. This enabled malware (ROCKSHOT) to infiltrate the system and cause the temperature control sensors to malfunction, while displaying the names of deceased migrant workers on QEWC workstations. Human rights groups have been critical of Qatar's treatment of migrant workers during the construction of World Cup facilities, which were mostly contracted out to Chinese firms. While the plant successfully leveraged reserves to stabilize water supply throughout the attack, unconfirmed sources reported panic buying of bottled water and water tanks running dry in migrant work camps.

QEWC hired Fenghuang Labs, a Beijing-based incident response firm, to assess the attack. Fenghuang discovered STANDINGPALM in the updated version of the Yuma software on which QEWC relies. Fenghuang attributed STANDINGPALM to the USG, based on its sophistication and alleged discovery of code that Chinese firms have previously associated with the USG. Fenghuang also discovered, but has not attributed, ROCKSHOT. Code for STANDINGPALM and ROCKSHOT remains closely guarded, making independent attribution and research difficult.

No other entity is known to possess ROCKSHOT, but plants in Chile, China and Morocco received the compromised Yuma software update containing STANDINGPALM. Despite the spread of STANDINGPALM, there are no other publicly reported disruptions. Following the release of Fenghuang's initial report, the French government privately expressed concerns to the USG about the potential role of the USG in the incident, stating it was reexamining its cybercrime-related coordination with the USG due to "irresponsible behavior." The Department of State offered immediate assistance to Qatar following the "brazen attack on civilian infrastructure."

## Incident Assessment

This attack on Qatari critical infrastructure (CI) coincided with the opening of the World Cup for maximum impact. The attack occurred on foreign soil but implicates US interests because of Qatar's strategic significance as a source of liquid natural gas (LNG) for the US, China, and Europe. Additionally, ROCKSHOT, which targets OT/ICSs underpinning CI, poses a potentially significant threat to the public health and safety of the American people and our national and economic security. The Pentagon alone relies on 2.5 million ICSs across all sixteen critical infrastructure sectors. The global threat of ICS exploitation from STANDINGPALM and ROCKSHOT could create humanitarian crises and severe economic disruption. The secrecy of Qatar and Fenghuang Labs impedes US efforts to mitigate the risk of future attacks and assist with a global response. Finally, Fenghuang's attribution of STANDINGPALM to the US threatens our global standing, alliances, and foreign policy objectives. The USG designation of this incident as either a "cyber incident" or "significant cyber incident," will determine available USG legal and policy options.

### Knowns

⇒ QEWC-hired Fenghuang Labs attributed STANDINGPALM (but not ROCKSHOT) to the US
⇒ The compromised Yuma update was also received by plants in Chile, China, and Morocco
⇒ Qatar is a major non-NATO ally of the US, a top BRI client for China, and strategic energy partner for both

### Unknowns

⇒ Whether the USG, US CI, or US private sector rely on compromised Yuma software
⇒ Technical aspects of STANDINGPALM and ROCKSHOT (*i.e.*, functionality, entry points, and origin)
⇒ The actors and motivation behind the QEWC attack (*e.g.*, UAE, human rights hacktivists, Russia, insider, anti-FIFA, etc.)

*Some policy options are dependent on investigative results and the outcomes of other policy options. Those recommendations have been designated as (conditional).*

## I. Investigate

### **Immediate** (72 hours)

***Domestic***

**1.1.1.** Request NSC emergency Cyber Response Group meeting to coordinate a whole-of-government response

**1.1.2.** Task ODNI with determining USG involvement or knowledge of STANDINGPALM and ROCKSHOT

**1.1.3.** Request CRG designate incident per Annex B of Cyber Incident Severity Schema, PPD-41

**1.1.4.** Direct NSA to conduct covert intelligence-gathering to obtain incident logs/malicious code samples from Qatar

*Risk: Detection, global outcry, assumed guilt*

**1.1.5.** Deploy the Software Bill of Materials as available to determine where Yuma is being leveraged throughout the government

***Global***

**1.1.6.** Request State to engage diplomatic channels to share information with France, Qatar, China, Chile, and Morocco (in hopes of obtaining STANDINGPALM & ROCKSHOT code)

**1.1.7.** Identify company that developed Yuma software to request code

**1.1.8.** Leverage US-Qatari 2018 MoU (between attorney general & Qatari counterpart) to request logs/code, IOCs, TTPs

### **Near-Term** (1-6 weeks)

***Domestic***

**1.2.1.** (*conditional*) Direct NSA to conduct forensic analysis on logs/code to determine TTPs, IOCs, and attribution

**1.2.2.** (*conditional)* Direct NSA to reverse engineer STANDINGPALM and ROCKSHOT

**1.2.3.** Request FBI keep close watch of cryptocurrency payments that could be linked to further propagation of ROCKSHOT

***Global***

**1.2.4.** (*conditional*) Request UK to leverage its 2014 MoU w/ Qatar to request logs/code

**1.2.5.** *(conditional)* Direct ODNI to conduct intelligence gathering operation to obtain STANDINGPALM, ROCKSHOT and understand accusation of US involvement from Fenghuang Labs

*Risk: Detection, global outcry, retaliation*

## II. Mitigate

### **Immediate** (72 hours)

***Domestic***

**2.1.1.** CISA issues a joint ICS-CERT Alert with the NSA, FBI, and DC3 to CI partners regarding compromised Yuma software, STANDINGPALM, and ROCKSHOT, advising firms to maintain backups, increase reserves and create redundant manual systems

**2.1.2.** The above-listed agencies in 2.1.1. issue a joint Alert regarding ROCKSHOT to the private sector

**2.1.3.** CISA coordinates response with key ISACs, covering critical infrastructure, emergency management response, and state, local & tribal governments

**2.1.4.** DC3 to remove Yuma software from Validations list for the DIB (if on list)

***Global***

**2.1.5.** US CERT to offer help to Q-CERT in Qatar

**2.1.6.** US CERT to offer help CSIRT (Chile) & maCERT (Morocco)

**2.1.7.** Engage Cyber Working Group of Gulf Cooperation Council to address vulnerabilities

### **Near-Term** (1-6 weeks)

***Domestic***

**2.2.1.** (*conditional*) Upon patch development, CISA issues update to previous Alerts

**2.2.2.** CISA to issue interim rule implementing Strengthening American Cybersecurity Act provisions mandating critical infrastructure partners notify CISA within 72 hours of a hack or ransomware payment

**2.2.3.** Designate any identified malicious actors under the Treasury-OFAC cyber-related sanctions program

***Global***

**2.2.4.** (*conditional*) US CERT makes patches open-source and available to affected nations

### **Long-Term** (2+ months)

***Domestic***

**2.3.1.** Implement interim rule for infrastructure resilience guidelines (NIST/NTIA)

**2.3.2.** CISA to engage in long-term outreach with CI partners relating to cyber protection and security, and voluntary reporting

**2.3.3.** CISA to work with Congress to establish cybersecurity investment tax credits to fund expert cybersecurity services for CI

***Global***

**2.3.4.** Request Treasury review CFIUS mandatory filing and review requirements for ICSs

## III. Communicate

### **Immediate** (72 hours)

***Domestic***

**3.1.1.** CISA director to issue public statement declaring no currently known threat to US systems, in order to maintain public calm

***Global***

**3.1.2.** Engage State diplomatic channels to reassure allies, like France, and partners Qatar, China, Chile, and Morocco

**3.1.3.** Issue statement through State commending QEWC for successful incident response to an actual cyber threat and swiftly mitigating the effects

**3.1.4.** State to issue statement urging caution relating to attribution and reiterating US commitment not to attack CI

### **Near-Term** (1-6 weeks)

***Domestic***

**3.2.1.** Encourage, through State and Commerce, technical repudiation of attribution in domestic and global outlets, specifically Al Jazeera

**3.2.2.** Encourage, through State, allies to issue statements echoing US call for caution on attribution

### **Long-Term** (2+ months)

***Global***

**3.3.1.** Commerce to promote Build Back Better World versus Belt & Road Initiative with allies and trade partners

**3.3.2.** Re-establish 2015 coordination systems between China & the US

*Risk: Political backlash, false security*

**3.3.3.** Increase funding for international cyber law enforcement and diplomatic trainings in key partner regions

**3.3.4.** Promote acceptance, specifically by China, of the UN GGE 2021 report on responsible state cyber behavior

## IV. Anticipate

### **Immediate** (72 hours)

***Domestic***

**4.1.1.** (*conditional)* Per PPD-41 cyber incident designation procedures, convene UCG to coordinate inter-agency action

**4.1.2.** Direct FEMA to place regional Incident Management Assistance Teams (IMATs) on alert for potential infrastructure crises in the US

### **Near-Term** (1-6 weeks)

***Global***

**4.2.1.** Alert CYBERCOM National Mission Teams to respond if requested by partner nations (i.e. Qatar, Chile, and Morocco

**4.2.2.** Direct USAID's OFDA to place Disaster Assistance Response Teams (DARTs) on alert for potential infrastructure crises in Qatar, Chile, Morocco, and China

### **Long-Term** (2+ months)

***Domestic***

**4.3.1.** Reform VEP process to take appropriate measures to counter cyber proliferation

***Global***

**4.3.2.** Invest, through DOJ, in information-sharing relationships with partner countries for future cyber incidents

**4.3.3.** Prepare punishments for non-compliance with norms of responsible state behavior set forth by UNGGE.