ZeroDarkNerdy Decision Document

EVENT SUMMARY
Findings from Fenghuang Labs (FL), a Beijing-based firm, indicate that on 21 November 2022, hackers targeted Qatar Electricity & Water Co. (QEWC) industrial control systems using a backdoor in Yuma software (STANDINGPALM) in addition to using destructive malware within the water plant (ROCKSHOT). As a result, QEWC needed to access reserve water resources due to higher volume demand during the 2022 FIFA World Cup in Doha. As part of their investigation of the incident, FL attributed this cyberattack to the United States, and listed China, Chile, and Morocco as other potential victims to a similar cyberattack.

	**Core** *Baseline - Near Term*	**Expansionary** *Longer Term*	**Escalatory**
Spread of Malware/Threat to US Infrastructure	• **CISA** to support US critical infrastructure to enhance its security protocols during this time. • **CISA** to develop contingency plan to ensure US could fend off similar attack in the future.	• **CISA, EPA** to investigate the vulnerability of IT/OT convergence with regard to US facilities and the presence of Yuma software. • **CISA's JCDC** to coordinate with the private sector to establish risk and response plans for water infrastructure. • Create a workforce development program by **CISA** to educate on vulnerabilities of water infrastructure.	• **CISA** acting through the **Department of State** to demand software analysis from Qatar and FL to secure US critical infrastructure.
International Reputational Impacts	• **Bureau of Cyberspace and Digital Policy** to reaffirm the US was NOT involved in QEWC cyberattack. • Continue to engage with French operations with the QEWC cyberattack.	• **State Department** to establish norm of information sharing.	• **NSA** to operate in greyspace to gain indicators of compromise from Qataris and FL. • Intelligence community to investigate connections between CCP and FL.
Regional Stability	• Offer **FBI** and **ODNI** investigative support to Qatar. • Encourage Qatar's NCA to enhance security at IT/OT convergence in critical infrastructure related to Yuma software.	• Recommend GCC to form cyberspace agency for confidence-building among members. • Provide capacity-building resources to heighten critical infrastructure security.	• Deploy US **CISA CSIRT** to Qatar to work with Ras Abu Fontas to prevent recurrence of similar cyberattacks.
US Citizens and Installations in Qatar	• Investigate if OT software is compromised in the Al Udeid Air Base. This would affect basic military functions and logistics.	• Place US citizens in Qatar on notice that they may need to evacuate. • Work with US citizens in Qatar to ensure access to water supplies.	• Direct Al Udeid Air Base to close itself off to all non-US citizens.
Humanitarian Concerns	• Direct **White House Press Secretary** to release a statement addressing domestic and international concerns about human rights.	• Encourage US sporting organizations to publicly release their own statements of the importance of labor rights and safety.	• Push Qatar to release a statement addressing international concerns about human rights concerns, specifically the migrant community.