



Cyber 9/12 Strategy Challenge

Intelligence Report I

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in late 2022. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform three tasks:

Written Situation Assessment and Policy Brief: Your first task is to write an analytical ‘policy brief’ that provides a concise assessment of the situation, addresses potential impacts and risks, and discusses the implications of the cyber incident. Describe policy considerations for different potential state and non-state actors. Be clear regarding the advantages and disadvantages of various policy options and explore the course of action you are recommending in depth. The length of the ‘policy brief’ is limited to **two single-sided pages**.

Oral Policy Brief (Day 1): For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

Decision Document (Day 1): Teams will also be required to submit a ‘decision document’ accompanying their oral presentation at the beginning of the competition round. The ‘decision document’ will be a maximum of one single-sided page in length, outlining the team’s response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written with the goal of assisting busy senior officials to quickly grasp your team’s recommendations and analysis.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in March 2022. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;

- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – Industry News Article
- **Tab 2** – Think Tank White Paper
- **Tab 3** – New York Times Article
- **Tab 4** – Ras Abu Fontas Email Chain
- **Tab 5** – Tweets
- **Tab 6** – Qatar News Agency Press Release
- **Tab 7** – Wired Article
- **Tab 8** – Diplomatic Cable
- **Tab 9** – Blogpost
- **Tab 10** – WAM Press Release
- **Tab 11** – State Department Press Release

INDUSTRIAL ENGINEERING



November 22, 2021
Eleanor Burhan

IT/OT convergence continues to streamline industrial processes

In 2015, a software firm named WenduView set up shop in Nanjing, China. The firm, established by a husband and wife, set their sights on developing software that could sense, monitor and report temperatures in power stations. WenduView is just one of many software firms developing software to be used in Industrial Control System (ICS) as a part of Operational Technology (OT). OT is comprised of both hardware and software that can detect or cause change in real-time, whether it's through to monitoring or control of a device or a process. Within OT, software plays a crucial role in the control and monitoring of systems and hardware, enabling real-time connectivity.

Unfortunately, this increased connectivity does come with increased risk to industrial processes that can range from the treatment of wastewater, to automated and computer-assisted manufacturing of consumer goods, such as automobiles and semiconductors.

OT can include functions, such as power generation and facility management, are often examined in a civilian context, it also enables basic functions and



support mission systems on government facilities and military bases around the world.

Governments and security experts alike are grappling with the challenge of adequately securing software-enabled ICS that is intrinsically tied to national security. One American expert estimates that in the United States alone, the Pentagon relies on an estimated [2.5 million](#) industrial control systems in hundreds of thousands of buildings.

Continued on Page 17.



THE LOUIS INSTITUTE
OF INTERNATIONAL
STUDIES



AT THE CROSSROADS:

China's Belt and Road Initiative in the Middle East PART ONE: THE GULF STATES

Foreign Affairs, “both parties agreed that the conditions are ripe to establish a [strategic partnership](#). We will accelerate the process and elevate bilateral relations to a new level.” This meeting illustrates the central role that the Middle East, and especially Persian Gulf States, play as a crossroads in China’s Belt and Road Initiative, and the absence of response to this evolving relationship by the United States and its Allies. This piece is second in an ongoing series, “China’s Belt and Road in the Gulf States: Investing at a crossroads.”

China’s Belt and Road Initiative (BRI), launched by President Xi Jinping in 2013, has been a cornerstone of Chinese state policy for almost a decade. The trillion-dollar initiative represents the cumulative effort of the Chinese state to build connectivity through investment and diplomacy in order to improve policy coordination, financial integration, as well as the connectivity of infrastructure, trade, and people across Asia, the Middle East, Africa, Europe, and even into Central and South America. As of December 2021, 145 countries have joined the BRI by signing a memorandum of understanding (MoU) with China, this number seeing the [largest growth](#) from 2016-2018. The BRI is not just an economic instrument, but is central to China’s efforts to increase its global reach and influence.

As of 2019, three countries on the Arabian Peninsula are among the top ten recipients of Chinese BRI investment, in terms of both the number and value of projects. The [value of BRI projects](#) in Qatar was second only to Russia by less than \$50 billion, and outstripped the other countries in the top ten by nearly \$100 billion. The Middle East region sits at a vital crossroads between Asia, Africa, and Europe. This key location, coupled with the region’s vast natural resources, mean that improving and stabilizing relations within in Middle East is central to the strategic implementation of the BRI. Gulf states, influential and energy-rich, are at the center of this strategy.

QATAR

The [Qatar National Vision 2030](#) maps the state’s long-term strategy focusing on human, social, economic, and environmental development. Fruition of this strategy will require continued significant development, both leveraging its status as an energy producer and decreasing its reliance on energy exports. Many of the Vision’s initiatives, as Chinese government officials have [messed](#) clearly, are in line with Chinese development priorities in the region.

The Chairman of the Federation of the Qatar Chamber of Commerce & Industry, and member of the Qatari royal family, Khalifa bin Jassim AlThani [stated](#) that part of his duty as chairman is to build commercial alliances to enhance Qatar-China relations. The Chamber pursues this policy via the exploration of opportunities to establish alliances and joint ventures between

Chinese and Qatari businesses as well as hosting an annual expo to encourage direct investment. The 'Made in China' expo is a forum for Chinese companies to make connections with their Qatari counterparts and exhibit their goods and services. Director-General Saleh bin Hamad al-Shaqi said that the trade fair was an invaluable opportunity to bring cutting-edge Chinese technology to the Qatari market in [sectors](#) ranging from construction and solar energy, to agriculture, desalination and medical devices. There are [more than 180](#) jointly owned Qatari-Chinese firms operating within the state, and in addition, due to laws allowing foreign investors 100% ownership, there are more than 14 Chinese-owned firms. Thanks in part to the effort of the Qatar Chamber of Commerce and Industry, Chinese technology has now been purchased by and integrated into the systems of an increasing number of Qatari companies across sectors.

One of the public centerpieces of Chinese investment and infrastructure cooperation is the Lusail Stadium, the home of the 2022 FIFA World Cup. China Railway Construction Corporation (CRCC) was chosen, in cooperation with Qatari contractor HBK Contracting, to build the 80,000-seat stadium – expected to be the largest stadium in the world. The stadium is located in the western edge of Lusail City, 20 kilometers north of Doha. CRCC is a large engineering contracting company with both [overseas and domestic contracts](#) spanning the construction of railways, highways, urban tracks, water conservancy and hydropower projects, buildings, municipal projects, bridges, tunnels, airports, and marine ports. Before construction began, the stadium's estimated worth was almost \$770 million – however reporting indicates that that prices tag has risen significantly over the course of construction, representing a significant but not dominant portion of the [estimated total of \\$220 billion](#) that it cost for Qatar to host the games.

In 2017 and 2018, China and Qatar signed a series of agreements and MoUs promoting cooperation in international commerce and global maritime investment, and cooperation is already significant in shipbuilding, manufacturing, petrochemicals, technology, hospitality, tourism, and financial services. A 2018 MoU was signed by the China Harbouring Engineering Company and QTerminals, the Qatari company that operates the Hamad port, and was intended to identify maritime investment opportunities for Chinese-Qatari cooperation. China Harbour Engineering Company, a subsidiary of Communications Construction Company which provides a wide range of infrastructure construction globally, was awarded the \$880 million contract in 2011. The China Harbouring Engineering Company was also involved in construction of the "Water Security Mega Reservoirs" scheme, taking part in the construction of 200 kilometers of pipeline connecting large water reservoirs to desalination plants and supply networks. Hamad Port is now one of the largest in the Middle East and its located just 40 km south of Doha. Since 2017, direct services have run between Hamad Port and Shanghai a trading line that helps Qatar lessen its dependence on its neighbors and helps stabilize and streamline oil exports to China.

Of central importance to China is Qatar's ability to supply the natural gas necessary to meet rising demand in China. In December 2021, the two countries signed another long-term

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

[contract](#), in a slew of deals around energy, stating that QatarEnergy would supply China, through Guangdong Energy Group Natural Gas Co, with 1 million tons of liquified natural gas (LNG) each year starting in 2024. This source of LNG is crucial not only for Chinese economic growth, but for strategic stability, as it lessens the country's reliance on energy imports from Saudi Arabia and Russia. Qatar has used its strategically significant position and assets the thread a fine line between cooperating with and profiting from both China and the United States. Leadership prefers to keep all energy related decisions independent, as evidenced by their departure from OPEC in January 2019.

Qatar's geographic location and energy resources are no less sought after by the US and Western countries. The growing Qatari-Chinese relationship, evidenced by recent deals with China and Chinese companies in and beyond energy, is of national and global security concern. Of particular disquiet is the import of the huge [Al Udeid](#) airbase in Qatar as a forward operating base for US Central Command. Though the US and NATO withdrew from Afghanistan and US strategic priority is largely pivoting eastward, the airbase is a crucial foothold in the Middle East. Europe is also increasingly interested in securing Qatar as a source of LNG. Russia has long been an unreliable energy supplier, especially in Eastern Europe. As countries across Europe look to diversify their energy suppliers to improve their resilience, increasing their share of LNG exported from Qatar would be a crucial step.

As the United States and Qatar celebrate 50 years of continuous dialogue, partnership, and long-term cooperation at this year's Policy Working Group meeting, the US must renew its appreciation of this relationship. US policy is shifting its focus toward China, but the BRI means that shifting focus to China means shifting focus to Chinese investments across the globe. China is implementing a long-term policy of economic expansionism that, little by little, is eroding US strength as a primary partner around the globe. The United States may not have a 'Belt and Road Initiative' but it does need to ensure that relationships with allies and partners around the world - like Qatar - remain strong.

The New York Times

Doha's shutdown of construction worker vigil resurfaces human right concerns ahead of World Cup

As preparations for the 2022 World Cup reach their final stages, continued challenges with migrant labor deaths illustrate a sobering picture of the wealthy petrostate.



By Katie Diangelo

Sep. 10, 2022

A small vigil for Abbas Khan, a Pakistani construction worker who died by dehydration, was swiftly shut down by Doha police last night, resulting in eight arrests, according to government sources. The arrests highlight ongoing concerns over migrant worker rights as the 2022 FIFA World Cup in Doha is set to begin in two months, on November 21.

Khan was one of approximately 20,000 Pakistani migrants to Qatar, the majority of whom work in the construction industry. It is unclear whether he was involved in the construction of Lusail Stadium, the location of the 2022 World Cup. If so, he would be one of over 6,750 migrant construction workers who have died in Qatar since the 2010 announcement of Doha's winning bid. At least 864 of those deaths were of Pakistani nationals, according to the Pakistani Embassy in Doha.

Concerns over migrant labor abuses in Qatar are not new. Of a population of 2.5 million, only 11.6% are Qatari nationals. The majority of non-nationals are migrant workers from South and Southeast Asia who often work in low-paid, labor-intensive industries such as construction and domestic care. Many pay large sums of money to recruitment agencies that promise higher salaries than workers ultimately receive. Until recently, employers could also seize workers' passports to prevent them from leaving or changing jobs without permission, under a system called *kafala*.

Many of the construction worker deaths are classified as being due to “natural causes,” without conducting full autopsies. Saarah Nahas of Amnesty International says that this categorization often hides the acute physical stress that many workers are under, especially in the summertime, and due to lack of access to basic necessities such as water, or adequate safety precautions. “Given that construction workers are often healthy, young men, we are certain that sudden deaths due to ‘natural causes’ misrepresent the actual cause of mortality,” says Nahas.

Local migrant aid groups generally agree with Nahas’s characterization, though they are often reticent to criticize the Qatari government publicly. An American expatriate who had befriended Khan while volunteering for an aid group noted that Khan had “complained about working conditions for months, but the construction company had done nothing. They swept it under the rug, like they always do.” Khan’s friend continued, “It’s ironic, isn’t it? Qatar has the highest per-capita water consumption in the world, and yet the workers that make the Doha lifestyle possible are dying of thirst on the job.” The expatriate requested to remain anonymous over concerns for his own safety.

Qatar disagrees with this characterization of migrant labor conditions. While the government does not dispute the number of deaths, only 37 have been officially linked to the construction of the stadium. Authorities claim that the rate of migrant worker deaths in the construction industry is consistent with broader trends in expatriate mortality in Qatar. They also note that death rates among migrant workers have dropped over time, due to stricter labor laws.

Concerns over migrant labor conditions were shared among participating football teams. Players from Denmark, Germany, and Norway have used their jerseys to display messages critical of labor abuse instead of sponsor logos.

FIFA, soccer’s international governing body, has taken a more conciliatory approach, recognizing that international scrutiny on Qatar due to the World Cup has prompted significant reforms to labor laws and regulations. Following intense international criticism and pressure, FIFA’s governing committee published the [FIFA Human Rights Policy](#) in 2017, which supports labor rights protections on stadium construction sites.

Facing international outcry, Doha has also taken steps to improve labor conditions. The Qatar Labor Law has been revised several times since the location of World Cup 2022 was announced. Significant amendments include implementation of a national minimum wage, stiffer penalties for violation of worker rights, and greater flexibility for workers to change employers.

Notably, the Supreme Committee for Delivery and Legacy, which is the national body responsible for overseeing the organization of World Cup, implemented stricter protections for laborers working directly on construction of the stadium. However, these protections do not apply to the thousands of other workers who were involved in

constructing other infrastructure that will support the influx of visitors during the tournament.

Yet, the recent vigil and subsequent arrests, continuing high rate of construction industry deaths, and lack of transparency in investigations related to migrant deaths demonstrate that Qatar has a long way to go in labor law reform.

“I was originally very excited when I heard that the World Cup would be hosted in the Middle East for the first time, but a lot of my friends back home don’t think I should go to the games,” said a British soccer fan living in Doha. “I hadn’t realized how bad the worker conditions were when I first moved here, and now I feel guilty contributing to it.”

He hasn’t decided whether he’ll watch the games on TV. “It’s supposed to be the world’s most beautiful game. I don’t know if I can completely miss it.”

Nahas hopes that the looming start of the games will bring back attention to Qatar’s continuing struggle with labor rights. “Our worst fear is that once the games are over, enforcement of the labor laws weaken and worker conditions deteriorate. We need to make sure that international scrutiny continues beyond the World Cup, as there’s still a long way to go until worker conditions are anything close to adequate.”

Tab 4 – Ras Abu Fontas Email Chain

From: Lennie Arias
Date: Monday, November 21, 2022 at 10:37 AM
To: Naima Barlow; Damian Klein
Cc: Rawan Hijazi
Subject: URGENT: Malfunction with Temp Control Sensors

Hey folks—happy monday

I'm noticing issues with the temperature control sensors. the long and short of it is that water yield is down so we're not able to meet demand at the moment.

Because the sensors aren't functioning as normal, the water temperature isn't getting high enough for desalination. Can we get a green light to manually override?

Lennie Arias
Security Analyst, IT Department
ext. 6520



شركة الكهرباء والماء القطرية
QATAR ELECTRICITY & WATER CO. Q.E.W.C.O.

From: Rawan Hijazi
Date: Monday, November 21, 2022 at 10:54 AM
To: Naima Barlow; Damian Klein; Lennie Arias; Aleks Povey
Subject: URGENT: Malfunction with Temp Control Sensors

Thanks for kicking off this chain, Lennie.

Unsure about overriding at the moment. A few minutes ago my computer screen went dark and this showed up:

ABBAS KHAN
SUJAN MIAH
YAM BAHADUR RANA
MANJUR KHA PATHAN
MOHAMMAD KAOCHAR KHAN
TUL BAHADUR GHARTI
RUPCHANDRA RUMBA

The same thing is showing up on other screens around the office. Looping in Aleks.

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

- R

Senior Security Analyst, IT Department
Sent from my iPhone, please excuse any typos

From: Naima Barlow
Date: Monday, November 21, 2022 at 10:58 AM
To: Rawan Hijazi; Damian Klein; Lennie Arias; Aleks Povey
Subject: URGENT: Malfunction with Temp Control Sensors

If water yield is down, could we tap into reserves? Demand has been high ahead of the games kicking off.

Naima Barlow
Security Analyst, IT Department
ext. 4823



شركة الكهرباء والماء القطرية
QATAR ELECTRICITY & WATER CO. Q.E.W.A.C.

From: Damian Klein
Date: Monday, November 21, 2022 at 11:02 AM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Aleks Povey
Subject: URGENT: Malfunction with Temp Control Sensors

We've increased reserves to be sufficient for close to a week, up from 48 hours. So it's an option. We still need management approval in order to tap into the reserves. Let me raise it with the higher ups.

Damian Klein
Water Systems Supervisor
ext. 7812



شركة الكهرباء والماء القطرية
QATAR ELECTRICITY & WATER CO. Q.E.W.A.C.

From: Aleks Povey
Date: Monday, November 21, 2022 at 11:04 AM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Damian Klein
Subject: URGENT: Malfunction with Temp Control Sensors

Hey folks Damian and I are looking into this, standby.

Aleks Povey
SOC Manager
ext. 1504



شركة الكهرباء والماء التطويرية ق.م.م.
QATAR ELECTRICITY & WATER CO. Q.E.W.A.C.

From: Damian Klein

Date: Monday, November 21, 2022 at 11:16 AM

To: Naima Barlow; Rawan Hijazi; Lennie Arias; Aleks Povey; Angela Goff

Subject: URGENT: Malfunction with Temp Control Sensors

Just got off the phone with Angela and the COO. We have the green light to tap into reserves. Copying Angela.

Damian Klein
Water Systems Supervisor
ext. 7812



شركة الكهرباء والماء التطويرية ق.م.م.
QATAR ELECTRICITY & WATER CO. Q.E.W.A.C.

From: Aleks Povey

Date: Monday, November 21, 2022 at 11:43 AM

To: Naima Barlow; Rawan Hijazi; Lennie Arias; Damian Klein; Angela Goff

Subject: URGENT: Malfunction with Temp Control Sensors

Something's definitely up. Flagging that we're likely going to lose some functionality before this is resolved.

Aleks Povey
SOC Manager
ext. 1504



شركة الكهرباء والماء التطويرية ق.م.م.
QATAR ELECTRICITY & WATER CO. Q.E.W.A.C.

From: Aleks Povey

Date: Monday, November 21, 2022 at 1:26 PM

To: Naima Barlow; Rawan Hijazi; Lennie Arias; Damian Klein; Angela Goff

Subject: URGENT: Malfunction with Temp Control Sensors

Quick update—looks like malware has been impacting temperature controls. It's beginning to spread. We'll need to isolate and restore from backups.

More to come.

- Aleks

Sent from my handheld device

From: Lennie Arias
Date: Monday, November 121, 2022 at 1:32 PM
To: Naima Barlow; Damian Klein; Aleks Povey; Angela Goff
Subject: URGENT: Malfunction with Temp Control Sensors

Should we prepare any public statements or warnings? In case we go through reserves.

Lennie Arias
Security Analyst, IT Department
ext. 6520



شركة الكهرباء والماء القطرية
QATAR ELECTRICITY & WATER CO. Q.E.W.C

From: Angela Goff
Date: Monday, November 21, 2022 at 1:41 PM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Damian Klein; Aleks Povey
Subject: URGENT: Malfunction with Temp Control Sensors

No--hold close.

We want to resolve this as quickly as possible and don't need to cause panic during the first day of the games. I've notified the executive office about this and will continue to provide periodic updates.

- AG

Angela Goff
Chief Information Security Officer
ext. 7262



شركة الكهرباء والماء القطرية
QATAR ELECTRICITY & WATER CO. Q.E.W.C

From: Aleks Povey
Date: Monday, November 21, 2022 at 9:43 PM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Damian Klein; Angela Goff
Subject: URGENT: Malfunction with Temp Control Sensors

Alright folks, we believe we were able to isolate the malware and restore from backups. temperature sensors are functioning again. We should be all good to resume operations momentarily. It'll take some time for us to get back to full operational capacity but we'll get there.

- Aleks
Sent from my handheld device

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: Damian Klein
Date: Monday, November 21, 2022 at 9:48 PM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Aleks Povey; Angela Goff
Subject: URGENT: Malfunction with Temp Control Sensors

Thanks Aleks. Angela and Aleks, confirming we can begin to replenish reserves?

Damian Klein
Water Systems Supervisor
ext. 7812



شركة الكهرباء والماء القطرية ق.م.س.
QATAR ELECTRICITY & WATER CO. QEWCO

From: Aleks Povey
Date: Monday, November 21, 2022 at 9:51 PM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Damian Klein; Angela Goff
Subject: URGENT: Malfunction with Temp Control Sensors

Confirmed.

- Aleks
Sent from my handheld device

From: Damian Klein
Date: Monday, November 21, 2022 at 9:53 PM
To: Naima Barlow; Rawan Hijazi; Lennie Arias; Aleks Povey; Angela Goff
Subject: URGENT: Malfunction with Temp Control Sensors

Thanks Aleks. I'll circle back with an ETA to fully replenish reserves. I think this will take longer than normal since we're not operating at 100% just yet.

Damian Klein
Water Systems Supervisor
ext. 7812



شركة الكهرباء والماء القطرية ق.م.س.
QATAR ELECTRICITY & WATER CO. QEWCO

From: Rawan Hijazi
Date: Monday, November 21, 2022 at 9:55 PM
To: Naima Barlow; Damian Klein; Lennie Arias; Aleks Povey; Angela Goff
Subject: URGENT: Malfunction with Temp Control Sensors

So I know this was close hold but it appears word got out that we were relying on reserves. My roommate sent me an article about some of the migrant communities running out of water. Some workers were hospitalized for dehydration. This isn't good.

- R

Senior Security Analyst, IT Department

Sent from my iPhone, please excuse any typos

From: Naima Barlow

Date: Monday, November 21, 2022 at 9:58 PM

To: Rawan Hijazi; Damian Klein; Lennie Arias; Aleks Povey; Angela Goff

Subject: URGENT: Malfunction with Temp Control Sensors

Oh no. Have you seen that video of people siphoning water from the irrigation canals near the stadium?

Naima Barlow

Security Analyst, IT Department

ext. 4823



شركة الكهرباء والماء القطرية
QATAR ELECTRICITY & WATER CO. Q.E.W.C.O.

Tab 5 – Tweets

 **mhmd**
@mo_abdulla777

Hearing rumors that #WorldCup2022 organizers are a lot more worried than @kahramaa is... this better not affect the players 🙄

1:46 PM · Nov 21, 2022 · Twitter for Android

4 Retweets 1 Quote Tweets 19 Likes

 **Brett B**
@aus2doh

Am i cursed? Can't believe i left Texas only to have to deal with water shortages AGAIN #worldcupwatergate

3:58 PM · Nov 21, 2022 · Twitter for iPhone

2 Retweets 1 Quote Tweets 49 Likes

 **Jessica Smith**
jessiesm

brb filling up my bathtub
[#worldcupwatergate](#)



4:26 PM · Nov 21, 2022 · Twitter for iPhone

3 Retweets 44 Likes

 **Khalid Ashraf**
@khashmoney_


Doha is no stranger to supply
disruptions 🙄🙄🙄 if we can airlift
cows we'll have no problem getting
water

5:13 PM · Nov 21, 2022 · Twitter for iPhone

2 Retweets 15 Likes





Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

 **Noora** ✨
@noora__al

@Carrefour_qa shelves are empty, local baqala is selling small bottles of water for 15 qar each. this is insane!

9:20 PM · Nov 21, 2022 · Twitter for iPhone

24 Retweets 5 Quote Tweets 87 Likes

 **KAHRAMAA** ✓
@kahramaa

We are pleased to announce that water production has been restored. Find our water resilience strategy and efforts to reduce Qatar's water consumption at #KahramaaMobileApp

10:02 PM · Nov 21, 2022 · Twitter Web App

5 Retweets 1 Quote Tweets 41 Likes

 **Ashwin Kumar**
@ashkumar

Just wanted to watch ⚽ not worry about basic necessities
#thisiswhywecan'thave nice things
#worldcupwatergate

10:18 PM · Nov 21, 2022 · Twitter for Android

6 Retweets 1 Quote Tweets 22 Likes

 **AI Jazeera Breaking News** ✓
AJENews

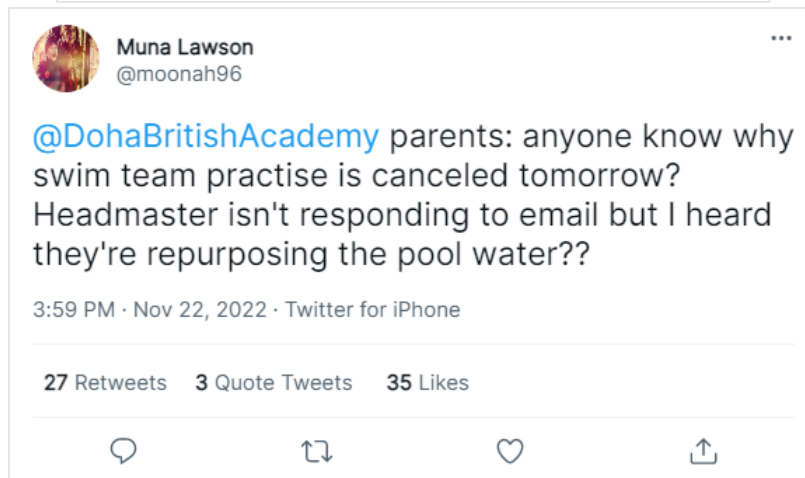
BREAKING NEWS: Online grocery shopping app Finstacart crashes as customers scramble to buy water. Read more: <https://bit.ly/3t4iWkO>



11:57 PM · Nov 21, 2022 · Twitter Web App

528 Retweets 1.1k Likes





Mariyah Al Hamdi 
@MariyahHRW




Received reports that water tanks in migrant worker camps near Doha ran dry and weren't replenished, hospitalizations due to possible dehydration. Camps weren't connected to water distribution pipelines, demand skyrocketed after QEWC cyberattack. Posting via @hrw once confirmed.

6:11 PM · Nov 25, 2022 · Twitter for Android

53 Retweets 14 Quote Tweets 210 Likes



Herald Sun 
@theheraldsun



Former FFA spokesman Oliver Vuon under fire for calling #Qatar water crisis "sweet, sweet karma" for alleged Qatari bribery to host #WorldCup2022, saying "Australia actually knows how to run an international competition." Details: <https://bit.ly/3BP3nkY>

12:16 PM · Nov 26, 2022 · Twitter Web App

30 Retweets 2 Quote Tweets 96 Likes



Tab 6 – Qatar News Agency Press Release



National Cybersecurity Agency chairman congratulates QEWC for rapid response and recovery from recent cyberattack

Doha, November 28 - A cyberattack at Ras Abu Fontas desalination plant was reported on 21 November. Despite a temporary disruption to desalinated water production, the plant was returned to normal operations within 11 hours, with no lasting impact to Qatar's water or electricity supply.

Abdulrahman Ali Al Farahid Al Maliki, Chairman of the National Cybersecurity Agency, congratulated Qatar Electricity and Water Company's (QEWC) rapid response and recovery from the cyberattack. "Like many countries around the world, Qatar recognizes that cyberattacks against critical infrastructure are becoming more common and has been working closely with our critical infrastructure partners to prepare for the possibility of cyberattacks during the World Cup. This is why QEWC was able to return to full operational capacity within only a few hours of the attack with no interruption to customers' water supply, even with the increased demand during World Cup events."

When asked about the ongoing bottled water shortage, he reiterated that there was no need for visitors or residents to stock up on water, as water reserves have been fully recovered since the incident.

Related: Doha residents queue for bottled water after rumored water shortages (Nov 24)
Related: MOFA "examining options" following attribution of QEWC cyberattack to the US (Dec 06)

He continued, "We have been preparing for a cyberattack against our water and electricity infrastructure for years. We require our desalination plants to have multiple failsafe mechanisms and expanded our water reserves in preparation for the World Cup. We've also implemented many initiatives for sustainable water management to make the 2022 World Cup in Doha the greenest ever. Our ability to respond and recover quickly from this attack proves that our cybersecurity measures have succeeded."

Chairman Al Maliki is collaborating with QEWC and the Electronic Security Unit of the World Cup 2022 Operations, Security and Safety Committee to ensure that the World Cup continues to operate smoothly. Qatar released its first National Cybersecurity Strategy in 2014. Establishment of the National Cybersecurity Agency is currently underway.

To report a cybersecurity incident, contact Qatar's National Information Security Center, Q-CERT, at incidents@qcet.org, or call +974 4493 3408. General inquiries can be directed to request-for-info@qcet.org.

MOST POPULAR

SEE PHOTOS: Today's World Cup matches (Updated Live)

World Cup an example of growing Qatari-China partnership

Qatar's growing role in the Gulf: Is the 2022 World Cup the start of a new era?

FIFA officials respond to resurfaced allegations of labor abuse

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

WIRED

SHERYL KEATING

SECURITY DEC 5, 2022

The US Might be Behind Attack on Qatari Desalination Plant

Nadia and her family keep their bulky, 5-liter water jugs in the same small closet where the washing machine hums. Linens and a sewing kit, stored in a Quality Street tin, were relocated to make room for the jugs in the family's three-bedroom apartment in Al Wakrah, Qatar, just 12 miles south of the country's capital of Doha. The jugs are new additions to the house, acquired after waiting an hour and a half in line at a local grocery store following news of a disruption at the Ras Abu Fontas Desalination Plant. From now on, Nadia promises that her family will always keep at least a 40-liter inventory of water.

The Ras Abu Fontas Desalination plant is the arid country's largest such plant, and news of a cyberattack at the plant last week has sent shock waves through the country, coinciding with the opening ceremonies of the long awaited (and long debated) FIFA World Cup. Residents of the peninsular country lined up alongside spooked soccer fans for hours outside grocery stores, convenience stores, and even public fountains in order to ensure their individual water supplies. Activities at the plant were disrupted for nearly half a day, and it took several more days to get operations at Ras Abu Fontas fully back to normal and water reserves in the country replenished to the levels before the attack. Nadia recounts her thinking that afternoon: "This is a hot place. We hear stories of people getting heat strokes, suffering from dehydration. We didn't know how long the attack would be taking place, and we didn't know if it would be the first of many. All we knew was 'we need water.'"

In the early stages of the attack, the plant's security and engineering teams noticed that temperature control sensors were not behaving properly, threatening the plant's ability to meet the country's water demands which were heightened as a result of the World Cup. As that was unfolding, devices around the plant became inoperable, instead displaying the names of migrant workers who have died in Qatar across the screen. The plant only saw operations completely return to normal – and water reserves replenished – several days following the attack; in the meantime, Qataris were left to wonder if the nation's scant water reserves would run dry.

The Qatari Electricity & Water Co., who run the Ras Abu Fontas plant, hired Fenghuang Labs to perform an autopsy of the attack. The Beijing-based incident response firm identified that the plant was using a compromised version of Yuma software that included a backdoor. Yuma software is common in desalination and water treatment plants around the globe, playing a critical role in regulating water temperature. The security team at Fenghuang Labs has dubbed the backdoor STANDINGPALM.

According to Pan Pengfei, a senior analyst at Fenghuang Labs, the discovery of the compromised update at Ras Abu Fontas is just the tip of the iceberg. “We have identified several additional victims, and we expect to uncover more as we continue to investigate.” The team at Fenghuang Labs indicated that plants using Yuma in China, Morocco, and Chile have also received the compromised update. This list is expected to grow as the investigation unfolds. Pan clarified that none of the other compromised entities have publicly reported disruptions.

Fenghuang Labs’ report named the US government as the force behind the STANDINGPALM as the sophistication of the backdoor points to the handiwork of nation-state hackers. “Attacks like this are uncommon,” Pan told Wired. “A lot of time and energy goes into infiltrating a software company such as Yuma, developing malicious code to sneak into an update, and successfully pushing that code out without anyone noticing.” Researchers also found notable instance of code reuse – when snippets of unique code are used across different software – between the code in the compromised update and past malware that Chinese firms have attributed to the US government.

In addition to the backdoor, Fenghuang Labs researchers also discovered destructive malware at the plant, which seems to be responsible for the actual disruption at the Ras Abu Fontas plant. This malware is what caused the plant’s temperature control sensors to malfunction while the screens of impacted devices displayed a homage to deceased migrant workers. Fenghuang Labs researchers have christened this malware ROCKSHOT. If the backdoor was the crowbar that opened the window, its brother ROCKSHOT was the one to start smashing things and painting graffiti on the walls. The incident is still under investigation, and Fenghuang Labs researchers have promised further updates as their work continues.

Rodrigo Gil, Head of Threat Hunting at industrial control systems (ICS) security firm MontSec and former NSA researcher, questions Fenghuang Labs’s analysis. “These are really big accusations to make,” Gil said over email, referring to the implication that the US government had access to the Ras Abu Fontas Desalination Plant and other such plants running the compromised version of Yuma. “There are things about this incident that don’t sit right with me. That’s really all I can say, since nothing is being shared. For such a big story, I would urge the [security] community to be skeptical until we see stronger public evidence to support that attribution [to the US government].” Fenghuang Labs have kept many of the details of the attack and investigation closely guarded, making it difficult for other researchers to conduct their own analysis.

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Much is still unknown about the attack on the Ras Abu Fontas Desalination Plant, however, the presence of a US government crafted backdoor on machines that serve such critical functions to society could represent a disturbing new trend. While analysts and policymakers hash out the details of what happened and plan next steps, Nadia will keep an eye on the water jugs she's saved for a not-so-rainy day.

Tab 8 – Diplomatic Cable

S E C R E T SECTION 01 OF 01 PARIS 204168

SUBJECT: U.S. and France Collaboration on Cyber Crime

DATE: DECEMBER 6, 2022

CLASSIFIED BY: U.S. Embassy Paris, U.S. Department of State REASON
5.1 (b)

1. Summary: This morning, the Ambassador met with a representative from the French National Police's Central Office for Combating Information and Communication Technology Crime (OCLCTIC). The purpose of the meeting was to discuss a recently-closed cybercrime case on which our respective governments had cooperated.

The OCLCTIC representative expressed concern over the recent incident at the Ras Abu Fontas desalination plant in Qatar and its potential connection to U.S. Government. Specifically, they conveyed that Paris would be monitoring developments on the investigation and reevaluating cooperation on cybercrime with Washington due to what it considers irresponsible behavior in cyberspace.

Tab 9 – Blogpost



Disruption at the Ras Abu Fontas Desalination Plant leaves the UAE – and Potentially the World Cup – in Hot (Cold?) Water

December 7, 2022 -- Jordan Handler

BREAKING - About two weeks ago, on November 22nd, a cyberattack at the Ras Abu Fontas Desalination Plant – one of Qatar’s largest desalination plants and a key piece of infrastructure supporting this year’s World Cup event – caused the plant to lose all functionality. The plant’s operations were halted for approximately 11 hours, although the plant was able to rely on leftover reserves to provide an uninterrupted supply of water to the event and the region. However, it took the plant more than four days to fully recover operations – and, publicly, this cyberattack resulted in widespread panic in the region and an increase in already flaming-hot geopolitical tensions.

Early claims regarding attribution are pointing towards an entity that readers may not be expecting – our own country! A Chinese incident response firm, Fenghuang Labs, has claimed that the United States’ intelligence is behind the incident – but this is blatantly false. The Chinese are incentivized to point fingers towards the United States – and we must push back. Although technical analysis of the event is still underway, I have been able to identify several technical and geopolitical indicators that have led me to believe that the actor behind this operation is affiliated with or an agent of the United Arab Emirates.

From my perspective, there are three major drivers that support my claim. First, I have received detailed forensic information from a credible source that the malware used in the operation shared distinct characteristics and TTPs (tactics, techniques, and procedures) with previous exploits originating from the UAE. Specifically, there were two specific technical drivers of this. First, the malware’s language settings were set to Khaleeji Arabic – a sign that the malicious actor behind this must be from the region. Additionally, the adversary used both PowerShell and Scheduled Tasks during their operation – techniques that we regularly see utilized by actors directly or loosely affiliated with the UAE.

Second, the 2017 al-Otaiba email leak established bad blood between Qatar and UAE and provides a striking geopolitical justification for such an operation. The leak, which was released by a group shadily named “Global Leaks,” seemed to [demonstrate](#) collaboration between an American think tank and the UAE on a campaign to downgrade the image and importance of Qatar as a regional and

global power, including collusion with journalists who have published articles accusing Qatar of supporting terrorism. Ex-Department of State official Belinda Numenor told me that, to this day, the UAE still believes that the Qatari government was responsible for this – and that they must pay.

If this wasn't enough justification, my third and final point brings us home. Right now, there are two seismically large events occurring simultaneously in the Middle East – the Expo 2020 in Dubai and the 2022 FIFA World Cup in Doha. Both events are incredibly important for the economic health and image of their respective host countries – yet the World Cup has significantly overshadowed the Expo. An economic and political analyst who has spent his entire career in the region but asked to remain nameless told me that we should not be underselling the importance of the Expo to the UAE – and that they would be willing to go to great steps to shift the narrative the narrative in a favorable way.

Although this analysis of this incident is still ongoing, I am perturbed by what I have seen in my research. We cannot let China point their fingers at us on the global stage regarding this incident. We are competing with them on every battlefield – infrastructure, foreign investment, space, etc. We cannot give China an inch – especially when it isn't our fault. The actor behind this operation is almost certainly affiliated with or an agent of the United Arab Emirates – and I intend to let the whole world know it.

Tab 10 – WAM Press Release



Thur 8-12-2022 20:30 PM

NESA responds to recent cyber incident in Qatar

ABU DHABI, 8th December, 2022 (WAM) – Today, Dr. Mahmood Al-Hamad, Executive Director of the United Arab Emirates National Electronic Security Authority (NESA) commented on a recent incident at Ras Abu Fontas desalination plant in Qatar.

“There has been much speculation around this incident, some of it, unfortunately, ill-informed. We are in touch with our Qatari neighbors and have offered support as they navigate this uncertain time and as football enthusiasts gather in Doha for the world’s most popular sporting event.”

Dr. Al-Hamad asked the press to allow professional incident responders to do their job and complete a thorough investigation of the incident at Ras Abu Fontas before jumping to conclusions.

“We must remain wary of conclusions drawn by outside parties without direct information from impacted organizations, relying on error-prone open source intelligence,” Dr. Al-Hamad stated.

WAM/Mona Aziz



U.S. DEPARTMENT *of* STATE

[Home](#) > [Office of the Spokesperson](#) > [Press Releases](#) > Statement on the Ras Abu Fontas cyberattack

Statement on the Ras Abu Fontas cyberattack

PRESS RELEASE

ALEXANDER BOWEN

DECEMBER 9, 2022

Following the cyber incident last month at the Ras Abu Fontas desalination plant in Doha, Qatar, the Biden Administration immediately offered assistance to the Qatari government to ensure the security of its critical desalination plants. The shutdown of the desalination plant, a brazen attack against civilian infrastructure, threatened the health of the citizens of Qatar and the thousands of people from all around the world attending the 2022 FIFA World Cup.

The administration is thankful that the plant, and the Qatari government, were prepared to respond in a timely manner to ensure no lasting impact to Qatar's water or electricity supply.

As President Biden said earlier this week, the United States and Qatar have coordinated closely on a wide range of regional and global issues for 50 years, and we believe that this partnership will continue to strengthen.

Cyber 9/12 Strategy Challenge

Intelligence Report II

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in late 2022. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform two tasks:

Oral Policy Brief (Day 2): For the second day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

Decision Document (Day 2): Teams will also be required to submit a ‘decision document’ accompanying their oral presentation at the beginning of the competition round. The ‘decision document’ will be a maximum of one single-sided page in length, outlining the team’s response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written with the goal of assisting busy senior officials to quickly grasp your team’s recommendations and analysis.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in March 2022. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – NSA Memo
- **Tab 2** – Tweets
- **Tab 3** – Washington Post Cybersecurity 202
- **Tab 4** – Jacobin Article
- **Tab 5** – Think Tank Registration Page

- **Tab 6** – Atlantic Council Fast Thinking
- **Tab 7** – Reuters Article

Tab 1 – NSA Memo



FOR: Director of the National Security Agency

Subject: Briefing notes for meeting with POTUS RE: Presence of USG cyber capabilities in Qatar

DATE: DECEMBER 07, 2022

SUMMARY: PENSIVEPENGUIN is a persistent access tool developed by the U.S. Government to support long-term strategic collection related to the People's Liberation Army military infrastructure. PENSIVEPENGUIN was used by a non-USG actor to install malware at a Qatari desalination plant. The unintentional presence of PENSIVEPENGUIN in Qatar is the result of Chinese technology transfer. **Request POTUS support to mitigate political tensions with Qatari leadership, which will facilitate collaborative incident analysis to determine risk to ongoing national collections objectives.**

(TS//SI//OC/NF/FISA)

Background/Context: On December 06, 2022, POTUS requested a briefing by the Director of NSA in response to Beijing-based incident response firm Fenghuang Labs' allegations that the U.S. Government was involved in a cyberattack impacting Qatari desalination systems. As Qatari civilian infrastructure is not included in national collections priorities, POTUS requested clarification of the United States' objectives in developing the capability and how it was found in Qatar.

Operational Objectives: PENSIVEPENGUIN was developed as a backdoor into industrial control systems (ICS) used by the People's Liberation Army to **support long-term collection objectives on Chinese military infrastructure, as part of the United States' doctrine of "Defend Forward."** The backdoor was intended to establish a foothold for intelligence-gathering in military installations near Taiwan, though it also facilitated access to all PLA installations that used the targeted software. PENSIVEPENGUIN could be used to install a malicious payload on PLA networks if the NSA received updated specified national security objectives.

The target was PLA vendor Nikara Solutions, Ltd.'s software Yuma, which controls temperature sensors in power and water generation systems. The persistent access capability was developed with USG support by an insider at Nikara and delivered to Nikara clients via a compromised software update. No additional capabilities were included in the compromised update.

Spillover to Qatar: **Qatar was not an intentional target of PENSIVEPENGUIN.** National collections objectives related to PENSIVEPENGUIN were limited to PLA installations. However, Nikara supplies operational technology to military and civilian clients both within China and among China's Belt and Road Initiative (BRI) partners, including Qatar. NSA has assessed with **HIGH** confidence that Nikara's participation in Chinese technology transfer via BRI likely resulted in unintended installation of PENSIVEPENGUIN on Qatari ICS.

Impact on national collections objectives: Exposure of PENSIVEPENGUIN in Fenghuang Labs' incident analysis of the Qatar incident poses a risk to the specified national collections objectives in PRC. NSA has assessed with **HIGH** confidence that Chinese authorities are aware of and likely taking steps to remove PENSIVEPENGUIN from affected systems, as well as auditing critical systems and networks for unauthorized activity. Impact on short-term collections objectives likely **MODERATE**, with **MODERATE** risks to diplomatic relations with PRC. NSA is reviewing other forms of persistent access supporting the specified collections objectives in PRC to determine long-term impact.

Recommendations:

1. Emphasize that Qatar is a key strategic partner of the United States and remains excluded from the specified national collection objective.
2. Request POTUS support in mitigating political tensions with Qatari leadership to facilitate cooperation with Qatari partners with respect to incident analysis, with internal objective of assessing impact on ongoing collections objectives in PRC.
3. Request State Department coordination of diplomatic response to PRC; offer NSA support where relevant.

Responses to Potential POTUS Questions:

- Who was the insider at Nikara?

PENSIVEPENGUIN was designed by a CIA asset. The asset, a software engineer at Nikara Solutions, is directly involved in the development of software updates. Asset is a U.S.-educated Chinese citizen who returned to China as part of the Thousand Talents Plan. CIA to provide additional details regarding the asset.

- Was USG responsible for the attack on the Qatari desalination plant?

NSA confirms that the attack on the Qatari desalination plant was **NOT** a U.S. Government operation. PENSIVEPENGUIN was used by an unknown actor to install a destructive payload that disrupted the operations of a desalination plant. The destructive payload was **NOT** designed by NSA. NSA is conducting analysis to support attribution.

- If NSA was not directly involved in the Qatari incident, how did the threat actor find PENSIVEPENGUIN?


NSA has not yet determined how the unknown threat actor discovered PENSIVEPENGUIN. Investigation is underway. Current analysis does **NOT** indicate a leak from USG.

- Is the UAE involved in the Qatari incident?

Current analysis of the destructive payload indicates **VERY LOW** confidence of UAE involvement in the incident.

[...]





Tab 2 – Tweets


 **Jordan Handler** @HotTakeHandler ...

Interested in learning more about the recent incident at Ras Abu Fontas Desalination plant in Qatar? Worried about how it may affect the World Cup? Check out my recent blog post where I connect the attack to Drum roll please.... the United Arab Emirates!!





12:24 PM · Dec 9, 2022 · Twitter for iPhone


1.2K Retweets 512 Quote Tweets 111k Likes





 **Jim Harry** @fishingking120 · Dec 9, 2022 ...


Thank you for the meaningful analysis Jordan! Always A+ work

   5 





 **Elaine Jorg** @DogMememes01 · Dec 10, 2022 ...


Wow! Bold move from UAE.

  1  12 





 **Simon Park** @SimonPark · Dec 10, 2022 ...


Are you sure this is enough information to make a confident attribution to UAE here? I would love to read some more about your justifications/technical analysis...

 4  25  691 





 **Senator Theo Cruis** @CruiseforCongres · Dec 10, 2022 ...


Happy to see good friend Jordan Handler back in the news where he belongs. This is a must-read article debunking China's baseless accusations about the US's role recent Qatar cyber attack. UAE is the real threat and must be held responsible!

 45  258  18.4K 





 **University of East Highland's M** @uehM · Dec 10, 2022 ...

Useful new analysis providing an alternative take on attribution in the recent Ras Abu Fontas Plant hack.

 2  14  84 

 **Jorge Hamminison** @ThinkTankJorge · Dec 11, 2022 ...

I have been preaching about the escalating tensions between these two countries for years. Their budding cyber rivalry has flown under the radar for too long.

 1  4  22 



MAJ Tyler Green (Retired) ✓
@MajTGreen



Important analysis here from renown cyber expert Jordan Handler. We cannot let states use their cyber powers at will to advance their own agendas, especially around international events like the World Cup – it is the United States’ job as the global leader to prevent and punish these kinds of activities. We **MUST** take action! [#rulesbasedorder](#)



Jordan Handler
@HotTakeHandler



Interested in learning more about the recent incident at Ras Abu Fontas Desalination plant in Qatar? Worried about how it may affect the World Cup? Check out my recent blog post where I connect the attack to Drum roll please.... the United Arab Emirates!!

12:24 PM · Dec 9, 2022 · Twitter for iPhone

1.2K Retweets **512** Quote Tweets **111k** Likes



7:35 AM · Dec 11, 2022 · Twitter Web App

897 Retweets **124** Quote Tweets **55k** Likes





Jeremy Strong @JeremyStrong · Dec 12, 2022

He designed this to help analysts with imperfect knowledge assign responsibility for a particular attack, or campaign of attacks, with more precision and transparency. This spectrum assigns ten categories, each marked by a different degree of responsibility, based on whether a nation ignores, abets, or conducts an attack.

The Spectrum of State Responsibility

1. **State-prohibited.** The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate.** The national government is cooperative but unable to stop the third-party attack
3. **State-ignored.** The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped.** Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated.** The national government coordinates third-party attackers such as by "suggesting" operational details
7. **State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed.** The national government conducts the attack using cyber forces under their direct control
10. **State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces

1 65 421



Jeremy Strong @JeremyStrong · Dec 12, 2022

I'd encourage folks to take a look at this and think about the nuance between different levels of state responsibility before pointing fingers at state-integrated entities for an op that could have been executed by one, disgruntled, unaffiliated individual. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/>

1 20 95

Chinese software company Nikara struggles to patch Yuma following cyberattack

By Reggie Tonon

December 16, 2022 at 7:50 a.m. EST

Welcome to The Cybersecurity 202! Less than a month ago, Qatar’s largest desalination plant, Ras Abu Fontas, was hit by a cyberattack on the first day of the 2022 FIFA World Cup. Though the Qatari government plant operators were able to restore plant function before water reserves were depleted, the incident sent shockwaves through Qatar and the international community – shock that only increased when initial reporting from the contracted cybersecurity firm investigating the incident indicated possible US involvement.

Immediately following the incident, a further investigation conducted by an incident response team hired by Qatari authorities discovered that the attackers were able to access the physical control systems of the plant through the Yuma software, made by a Chinese company, Nikara Solutions, Ltd. and used by the plant as its centralized monitoring and control system. Subsequent investigation from Fenghuang, a Beijing-based cybersecurity company that specializes in incident response, attributed the compromised update, called STANDINGPALM, to the United States - attribution that has subsequently been contested by the US government.

Not long after this announcement was made, companies across Asia and Africa who use Yuma software began experiencing rolling disruptions. These incidents impacting an array of companies and in different regions, based on initial reporting, seem to be taking different forms. Once an entity uses the known vulnerability to gain a foothold in the target network, they have a wide range of exploitation options, from ransomware to data corruption and theft.

Nikara CEO, Su Runin, immediately announced that Nikara was working on a patch for the vulnerability with the support of the Chinese government, and that it would be made available immediately to those affected. A statement issued from the Cyberspace Administration of China emphasized the importance of this patch, and condemned the attack as “an irresponsible and dangerous” act.



The patch was in fact created and distributed with impressive speed within China beginning December 12. However, it appears that the majority of firms affected by this vulnerability outside China have not yet received the necessary update. Many Chinese companies that use this software within China are regarded as critical infrastructure, and thus likely have been prioritized the patch for national security purposes.

But in addition, it appears that Nikara is having difficulties rolling out the patch. Separated client lists, secondary users, and language barriers have all impeded the company's effort to remediate the situation.

This delay is not helping the growing discontent from impacted organizations across Africa and southern Asia who feel that once again they are caught in the crosshairs of global powers. Over the past day the hashtag #ThirdworldThirdway has been trending on twitter, as twitter users around the world try to bring attention to this cyber operation and yet another instance in which the 'Third world' are the ones suffering the consequences of the disagreements of global powers, and calling for countries and populations to bind together to disavow the binary choice of China- or US-aligned.



Global South Pays the Price for US-China Competition

BY
Henry Jones, Jr.

American leaders will tell you that the US-China great power rivalry is about democracy's fight against authoritarianism. This isn't true.

What they won't say is that capitalist competition, above all else, is driving tensions.



High-speed rail in Indonesia. Hydroelectric power stations in Uganda. A nuclear plant in Argentina. A military base in Djibouti.

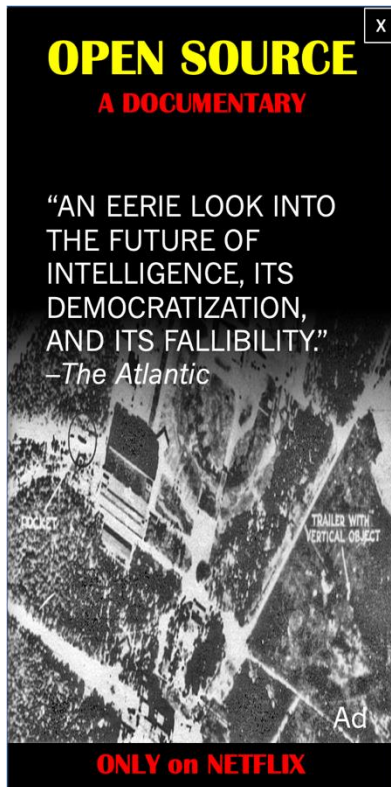
What do these have in common? They're all projects financed by the Belt and Road Initiative (BRI), a Chinese government strategy to invest in infrastructure development around the world. The BRI is the focal point of Chinese foreign policy.

China is looking to increase its standing and leadership in a world that the United States has dominated as the lone superpower since the end of the Cold War. Beijing seeks to challenge the United States and overturn an international political order carefully constructed to sustain and protect US hegemony. To do so, Beijing has sought to strengthen its relationships with governments through the BRI's funding of projects around the world, but primarily in the Global South, to facilitate economic development.

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

Skeptics of the BRI say that, through these investments, China is engaging in debt-trap diplomacy to gain political and strategic leverage over debtor countries.



And the skeptics may have a point. The terms of China's BRI loans are opaque and often difficult to meet for receiving countries. Vulnerable countries, already struggling financially, that are on the receiving end of billions of dollars in infrastructure investments can fall into serious problems if they fail to repay their debts. When most of that debt is owed to a single creditor, like China, the creditor can exert its influence to further its foreign policy objectives.

The United States for its part has advanced its own strategy to counter the BRI, the Free and Open Indo-Pacific Strategy, which emphasizes security, economics, and governance. This strategy purports to be centered around democratic ideals, but its similarities to that of China's is striking. US foreign direct investment in Asia Pacific Economic Cooperation (APEC) economies totaled over \$1.4 trillion in 2018 alone, according the Office of the United States Trade Representative.

The US-China rivalry shows few signs of letting up anytime soon. American businesses, especially banks, are affected greatly by Chinese state-owned companies squeezing them out of international markets by undercutting them.

Governments around the world, especially those of developing countries, are forced to decide on which capitalist giant to link their future fortunes—China or the United States.

What is clear is that these two countries are more concerned with capitalistic competition and vying for global influence than the needs of vulnerable states. The vulnerable, as they have throughout history, will continue to be exploited and caught in the crossfire of greedy, imperialist rivals.

ABOUT THE AUTHOR

Dr. Henry Jones, Jr. is a professor in the Department of Asian Studies at Marshall College.



All eyes on Doha: The aftermath of **STANDINGPALM**

THURSDAY, DECEMBER 15, 2022 | 12:30 PM ET

Please join the DC Institute for Policy Analysis for a public discussion on the cyberattack of a Qatari desalination plant ahead of the 2022 FIFA World Cup. On November 21, 2022, Ras Abu Fontas desalination facility in Qatar became the victim of a cyberattack just as the World Cup commenced. A compromised update for software controlling an important desalination plant prevented the treatment of water in an arid country and at a time when thousands of tourists have increased the demand for water. While short-lived, the incident prompted panic and its aftereffects still resonate throughout the world.

[REGISTER](#)

On December 5, Fenghuang attributed the incident to the US government. Since the incident, Nikara Solutions Ltd., the developer of Yuma software, has lagged on the deployment of its patch beyond China. Meanwhile, opportunistic criminal groups have taken advantage of the backdoor, **STANDINGPALM**, to target software used in everything from water treatment facilities to power plants, with a disproportionate impact on infrastructure in the Global South.

One of the groups taking advantage of this sudden free-for-all is The People's Militia, an anti-capitalist activist group believed to be based in the United States that has resurfaced for the first time since 2019. The People's Militia have a track record of cyber capability acquisition and use informed by edge-case ideologies of domestic militancy in the United States. The use of this now-public vulnerability has impacted infrastructure in Sub-Saharan Africa linked to China's Belt and Road Initiative.

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Tab 6 – Atlantic Council Fast Thinking



FAST THINKING: Macron criticizes US actions in cyberspace

JUST IN

French President Emmanuel Macron railed against recent US cyber actions in Qatar and other countries, stating “We condemn in the strongest terms the abuse of cyberspace to foment conflict in the absence of threat. There is no legitimate reason for a foreign government to harm the critical infrastructure of another state during peacetime. It is an inexplicable violation of international law to say little of the sovereign and unshakeable authority of a government over its own territory.” Allegations of US involvement in a recent incident at a water desalination plant in Qatar have provoked new divisions between the US and its European Allies and Partners. Our experts weigh in on the gravity of these actions and its consequences for Transatlantic cooperation.

TODAY’S EXPERT REACTION COURTESY OF

- Martina Petrovich, Deputy Director of the Center on European Affairs
- Andrei Aksenov, fellow and lead of malware research at Fox-IT
- Tony Raleigh, Senior Fellow with the Brzezinski Center and frmr Department of Defense official
- Lidia Solis, Associate Director at the Cyber Statecraft Initiative

Macron’s Position

- Since knowledge of (alleged) US cyber prepositioning has come to light, many governments have been quiet on a rather surprising discovery. Macron’s declaration “provides the first clearly articulated counterpoint to US strategy in cyberspace from a nominal ally,” say Martina Petrovich.
- France just wrapped up its stint in the presidency of the Council of the European Union, where one of the country’s focuses in that leadership role was cyber resilience across Europe. Lidia Solis notes, “France is very aware of these issues right now and is more ready to engage in conversation and debate than in years prior.”
- Martina further remarks that Macron is coming off a bruising reelection campaign where critics blamed the incumbent for a perceived decline in French prestige both within Europe and internationally, including the recent withdrawal of French forces from Mali, quickly replaced by an aggressive Russian presence. Playing hardball with countries such as the US could help Macron’s *En Marche* party push back against this narrative and strengthen its odds of claiming an absolute majority in the French National Assembly.

Implications for Defend Forward

- It’s time to see if France will walk the walk. Lidia Solis says, “these next few months will prove interesting if France does decide to press this issue and pressure the US to reevaluate cyber operations like this.” The implications of how Defend Forward is viewed

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

and implemented are particularly grand, though if France wants to pressure the US to abandon their current course, they will need to build a coalition of like-minded states to help turn up the heat.

- “If this is what Defend Forward looks like, then it’s making cyberspace less secure instead of more secure,” argues Andrei Aksenov. “Introducing instability into the cyber ecosystem – especially if, as it seems, there’s no strong control over the instability that’s been introduced – shows a disturbing lack of foresight.” There must be a more mature, disciplined approach in which the US is better able to monitor and curate its targets.
- Andrei points to challenges that Nikara Solutions is encountering while trying to rollout a fix to the compromised software. “The knock-on effects of this operation are wild. We need to ask ourselves now: does the US or its allies ever want to be part of a mess like this again?”
- Tony Raleigh, however, points to such efforts as the future. “Though this particular incident seems to have gotten out of hand, it is encouraging to see Defend Forward in action. The intention here is clear, though the spillover effects must be better managed in the future.”

The Future of Cyber Operations?

- Tony sees such activity as likely becoming the norm. “This is a necessary and logical step towards preparing the US for future conflicts. Just because you have access to a desalination plant or a power plant doesn’t mean you’re going to use it. Access to your adversaries’ networks is table stakes in the cyber domain. You can’t walk into many rooms if you haven’t opened the door- there is no forced entry in cyberspace. Our military and intelligence professionals have to be able to jump into action at a moment’s notice.” Tony notes that it would be “shocking” if the US were the only country engaging in such activity.
- Martina is hesitant as to whether acting solo on this is the best approach. “It begs the question: In which cases should we be involving our allies, and in which cases should we be acting alone?” Many desalination plants running the compromised software – and suffering disruptions as a result – are based in former French colonies, countries that France works to maintain close relations with. “One can see why Macron finds this frustrating and even a little embarrassing.”
- Andrei Aksenov asserts that such preemptive prepositioning is likely a hush-hush norm. “The French may not like it publicly, but they are certainly discussing leveraging it privately.” The right move might be to alert and onboard allies into such operations at an earlier phase.
- Lidia notes though that developing these capabilities might not be an effective use of resources, especially given the sorry state of cybersecurity at home for the US. “Cyber operations like this are sexy, but the real work needs to be done at building resilience at home. This is like the US breaking into people’s houses while leaving its own front door wide open.” Lidia points to the SolarWinds attack, in which thousands of organizations – many of them based in the US – were impacted by a compromised update themselves; the attack has been attributed by some to a Russian intelligence operation. “Let’s start closing some of these doors.”

Tab 7 – Reuters Article



TECHNOLOGY & CYBER SECURITY

DECEMBER 17, 2022 / 2:34 PM / UPDATED 3 HOURS AGO

American citizen implicated in Qatar water hacking

By Jocelyn Tan

2 MIN READ



DOHA – An American citizen has been identified as the culprit who helped launch a serious cyberattack against Qatar’s Ras Abu Fontas desalination plant in a cyberattack that coincided with the start of the 2022 World Cup last month. According to two law enforcement officials who asked to remain anonymous due to the ongoing investigation, as well as a Western intelligence official, the suspect shared highly sensitive information about the plant’s ongoing digital modernization efforts with an activist group that used it to design malware targeting Chinese components of desalination equipment. Sources believe that the activist group had leveraged the suspect’s existing sympathies for the large South Asian migrant worker community in Qatar to convince him to share expertise about the Ras Abu Fontas plant.



Qatari authorities have the man in custody but have not released his name. They confirmed the suspect is of South Asian descent and had volunteered within the migrant labor community as an expatriate in Doha.

Anonymous sources were able to provide additional details: the suspect had volunteered as an English and computer instructor since at least 2016 for a non-profit organization supporting migrant workers living in HBK Contracting’s worker accommodations. Over time, he had become friends with some of his students. He had also likely interacted with members of the activist group implicated in the attack, who may have posed as volunteers in the same non-profit organization.

Sources close to the suspect claim that while he had been sympathetic to the activists’ cause, he had not been willing to directly contribute until September of this year. They believe that the death of one of his students in late August due to dehydration, lack of thorough investigation by Qatari authorities, and the arrest of several other workers during a small vigil held in the deceased’s honor may have prompted him to act. However, they also believe the suspect was under the impression that the attack would consist only of defacement, not disruption to water production.

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

Note: All materials included are fictional, unless otherwise marked, and were created for the purpose of this competition. Any resemblance to real persons, organizations, or events is coincidental. All scenario content is the intellectual property of the Atlantic Council unless otherwise specified in writing. This content is licensed for use by our Cyber 9/12 competition partners and students competing in our Cyber 9/12 competitions without fee or compensation, and to all other parties with the written consent of the Atlantic Council. This scenario is developed for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

The suspect in custody was an employee at Qatar Energy and Water Corporation's (QEWC) Ras Abu Fontas desalination plant, one of the largest desalination plants in Qatar. According to a source at the QEWC, this individual was a project leader in the plant's continued effort to bring more modern digital technology into use across the facility. He had extensive access to design documentation and networks across the facility as different sectors of the plant were modernized over the previous 18 months. Due to the complex security protocols in place, QEWC claims that his sensitive access and expertise was critical for the success of the cyberattack against the plant. QEWC has since released a statement committing to improving security practices related to insider threats.

The November 21 cyberattack disrupted desalination at the plant for 11 hours, forcing Qatar to rely on water reserves to meet increased demand. Qatar's water supply has since recovered to normal levels. Qatar relies on desalination for approximately [60 percent](#) of its freshwater supplies.

While the World Cup was able to continue uninterrupted, the attack reportedly caused panic-buying and hoarding of bottled water among Doha residents and visitors.

Don Withall, the Director of Investigations within the Cybersecurity and Infrastructure Security Agency within the United States Department of Homeland Security, says that U.S. authorities have been coordinating with Qatari authorities to determine next steps.

"We are committed to the security of critical infrastructure in the United States and partners and allies across the world. The Department is working closely with law enforcement colleagues here in Washington and Doha to ensure that this individual is held responsible for his actions," he said.

Withall stressed that the U.S. is dedicated to upholding the highest standards of cybercrime enforcement.

Cyber 9/12 Strategy Challenge

Intelligence Report III

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the National Security Council (NSC). This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in late 2022. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The NSC needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the NSC.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform one task:

Oral Policy Brief (Day 2): For the final round of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the NSC.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

- *Don't fight the scenario.* Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in March 2022. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the NSC requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the NSC can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the NSC:

- **Tab 1** – Rabinara Group Report
- **Tab 2** – Statement from The People's Militia
- **Tab 3** – Foreign Policy Article

Tab 1 – Rabinara Group Report



Shedding Light on STANDINGPALM

DEC 19, 2022 | 5 MIN READ

Introduction

Rabinara Group has released details on the compromised Yuma software update that halted operations at the Qatari Ras Abu Fontas desalination facility during the 2022 FIFA World Cup in Doha. The incident impacted water treatment operations at the Ras Abu Fontas facility for 11 hours, requiring staff to utilize reserves to meet the increased demand for water. Following the incident, Fenghuang Labs, attributed the attack to the United States government (USG). Shortly thereafter, a now-debunked article published by Jordan Handler, an open source analyst, linked the incident to an actor connected to the government of the United Arab Emirates.

Analysis of Attacker Intent

Rabinara Group has finalized an investigation into this incident and assesses with high confidence that USG likely planted STANDINGPALM, a backdoor in Yuma software, to obtain access to Chinese military facilities, many of which rely on Yuma software. The malware, dubbed ROCKSHOT, that impacted systems at Ras Abu Fontas are assessed with high confidence to likely be linked to a US-based group which has been identified before but does not overlap with any activity groups linked to the US government.

The US-based group was able to remain persistent with the use of legitimate credentials, facilitating their access to the compromised environment and utilize the USG-planted backdoor. The intent of this second, US-based group, remains unclear at this moment. As devices at Ras Abu Fontas displayed the names of migrant workers who had died in Qatar, the group may have a motivation linked to activism.

[READ MORE](#)

Tab 2 – Statement from The People’s Militia



The People’s Militia @TPM2915102 4h
#micdrop

As staff at the plant scrambled to respond to a cyberattack against Qatar’s largest desalination plant, their screens no longer showed technical readouts or internal messages, but a never-ending scroll of the names of Qatar’s unjustly murdered. Migrant workers, who in Qatar are treated little better than slaves, come to the country seeking a better life but many instead find their death in the relentless heat – desperate for water. The overwhelming message we send to our brothers in behaving in such a cruel fashion is the value of human life has plummeted while the wealth of a few has risen higher than the clouds.

But where is that water going instead? To the capitalist congregation in Lusail, so that the plutocrats of the world can praise themselves for spending billions of dollars while the poor die of heat and thirst. From the sprawling royalty of Qatar to the oligarchs of Russia to the technocrats of the United States, no professed variance in ideology could overcome the base greed of the global elite.

Within Qatar there are few that empathize, or even see, the plight of the migrant workers. But at secret vigils and trips to worker camps we found those few. Including one who, born of South Asian immigrants and trained in the West, understood our mission and was in the position to bring it to fruition. These are the true global citizens, a constituency no more visible than the harms and horrors they suffer. We joined forces, pairing our understanding of insecure operational technologies with an insider sympathetic to our cause. It was through his access and intimate knowledge that we, at the moment the first whistle was blown to commence the ruthless extravagance, launched an attack on the Ras Abu Fontas desalination plant. Using a backdoor so kindly introduced by American jingoists and techniques practiced by Qatar’s doppelganger in exploitation, the United Arab Emirates, we nearly ground production of drinkable water to a stop.

Ours is not a place to struggle but to triumph over a small and concentrated minority stripping away the wealth and lifeblood of billions of souls across this Earth. We recognize that the weakness in the software provided by Qatar’s Chinese neo-colonizers, means that our action could be given life by others less ready to undertake the struggle and grow to not only expose the rank hypocrisy of the world elite congregating in Qatar, but the injustice of the entire global order. Our word is on the wind and our ranks grow daily. Today we have released knowledge of the backdoor, the representation of the global power struggle trampling the world, back to the people. Take up arms against those that may suppress your humanity, might charge you to draw breath on our collective blue dot, and find the power of this cyberspace to free yourselves from the tyranny of ritualized institutional oppression. Let any man take on these giants, and bring them crashing to the ground.

We have reminded the world that the wealthy and the powerful can yet be throttled. And we are far from finished.

Tab 3 – Foreign Policy Article



ANALYSIS

France calls on Brussels to cease cybersecurity cooperation with Washington

December 24, 2022

In a marked escalation, French policymakers called to cease all cooperation with the US on issues regarding cyber operations and cybersecurity. The move comes after weeks of back-and-forth between the two countries following revelations of a US cyber program designed to surreptitiously gain and maintain access to important targets, a program which Paris claims is both provocative and dangerous. “There are the norms we must safeguard now in order to ensure we stand back from the edge of that slippery slope,” French politician Fabian Cohen stated.

Not only is France shuttering its collaboration on cyber issues with the US, but it is pressuring Brussels to follow suit. While the peacetime prepositioning of malware in important entities has been seen before – in 2020, it was revealed that Russian intelligence had used a similar technique to gain access to tens of thousands of companies that used the IT management software SolarWinds – seeing the unintended consequences of such an operation has given the French pause.

The problem isn’t solely that the US has such capabilities, but that they lost track of and then lost control of the backdoor that had been implanted in software used by desalination plants around the world. The US has denied that they were aware that the Qatari desalination plant had received the compromised update, and an investigation is ongoing into how the hacker collective that caused the disruption at the plant – dubbed “The People’s Militia” – may have uncovered the backdoor. “It is in fact more, not less, disturbing that the US says there wasn’t knowledge that the backdoor had found its way to Qatar, and yet even more disturbing that a hacktivist group was able to take advantage of such an NSA-developed malware,” Cohen said. The incident has been branded in the French media as an irresponsible slipup on the part of the US government.

France is calling for an immediate suspension of all collaboration between the European Union and the United States, stating that such an incident indicates that US intelligence objectives are unrestrained, non-proportional, and contribute generally to global cyber-insecurity. Such a halt to collaboration could throw a serious wrench into the [US’s Defend Forward strategy](#) in

Cyber 9/12 Strategy Challenge | 2022 Washington, DC Intelligence Reports 1-3

cyberspace, which calls for the US to “proactively observe, pursue, and counter adversaries’ operations and impose costs short of armed conflict.” If European allies refuse to get on board, the US will have to decide whether to proceed alone or change course.

While France’s response likely driven by real concerns about irresponsible cyber operations, former French colonies have also been hit hard by STANDINGPALM. Desalination plants in Algeria and Lebanon were also found to have been infected with the US-made malware that was first discovered in Qatar, though it’s unclear if those plants have also experienced disruptions.