

A glowing lightbulb with a cracked glass globe inside, surrounded by falling glass shards. The lightbulb is illuminated from within, casting a warm glow. The globe is cracked and shattering, with many small pieces of glass floating around it. The background is a dark blue gradient.

Geneva Cyber 9/12 Strategy Challenge

ANEB JAK I „NUKE THEM“
MŮŽE BÝT ŘEŠENÍM
KYBERNETICKÉ KRIZE

KDO JSME?

- Anna Blechová
- Michaela Prucková
- Dominik Zachar
- Jakub Vostoupal

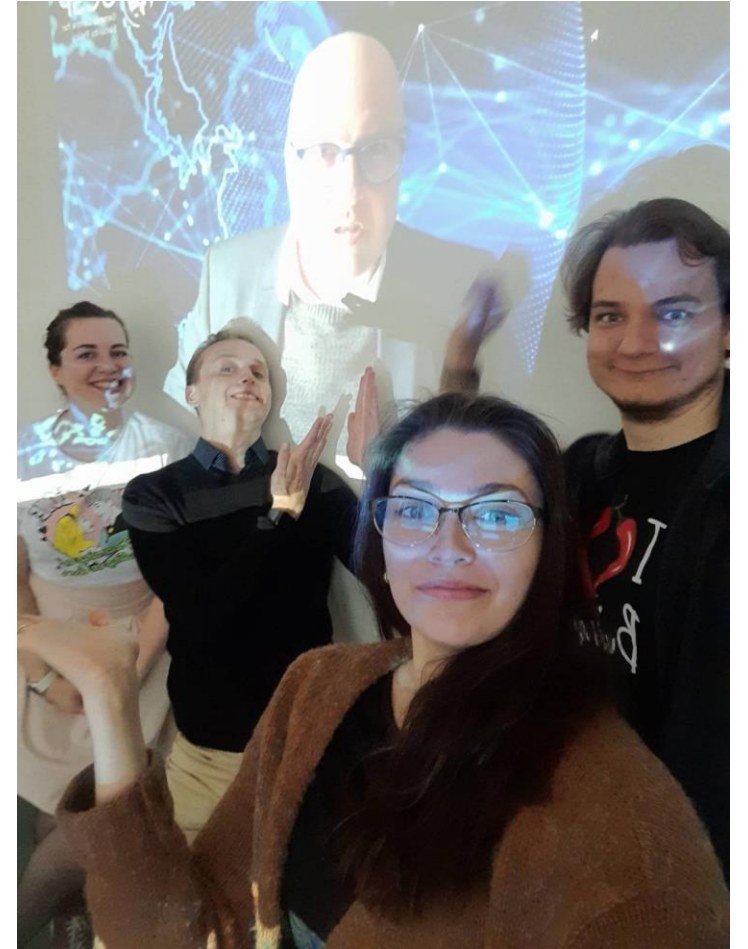
- 2021 - Cybertarians (Dr. Jakub Drmola)

- 2022 - Nuke them, Cybertarians!
(Dr. Jakub Harašta)



CYBER 9/12 STRATEGY CHALLENGE

- Atlantic Council
- Vícesto lokací (Washington, London, Geneva, Cynberra, Lille)
- Geneva Centre for Security Policy
- Virtuální prostředí
- Každoroční strategicko-politická soutěž pro studenty z celého světa
- Konfrontace fiktivní kybernetické krize založené v reálném prostředí
- Úkol? Vytvořit briefing a doporučení pro politickou reprezentaci a zabránit eskalaci



FUNGOVÁNÍ SOUTĚŽE

- Scénářové cvičení - Table-top
- Národní kola - ČR (?)
- Mezinárodní kolo
 1. **Kvalifikace (Důležitost CySec, co považujeme za aktuální výzvu a složení týmu)**
 2. **Písemné kolo - Written Policy Brief, 500 slov**
 3. **Ústní kolo a *decision* dokument**
 4. **Semifinále - 2. ústní kolo (+ *decision* dokument)**
 5. **Finále - 3. ústní kolo pod dozorem rozhodčích**

CSSC 2021

- Fiktivní země Nistria v EU, původně součástí království Mustelus
- Celosvětová pandemie COVID-21, panevropský medicinský systém
- Kyberincident v jedné z hlavních nemocnic Nistrie, postupné zpomalování systémů až kompletní kolaps, protivládní demonstrace
- Ekoteroristická skupina, royalisté, chyba, útok další strany...
- **Eskalace:** Zpomalování systémů v dalších nemocnicích, přetékání do panevropského systému, stávky personálu, eskalace pandemie
- **Finále:** Celkový kolaps panevropského systému

CSSC 2022

- Fiktivní země Nistria v AU a sousední království Mustelus, podobnost s RF čistě náhodná, Miraba
- African Union Directorate of Cyber Security (pan-African CERT)
- Velká závislost na mobilních platebních službách a satelitech, hornaté prostředí, těžba Germania (polovodič), politické pnutí mezi Nistria a Mustelusem
- Postižení platebního systému, chybovost transakcí, ztracený kontakt se severem země, zasažení satelitů
- Royalistické tendence, zhoršování vztahů s Mustelusem i dodavatelem satelitních služeb, špatná komunikace vlády směrem k lidem
- **Eskalace:** zával horníků, rozšíření incidentu na banky => hrozící pád bankovního sektoru, fake news

NÁSTIN ŘEŠENÍ

- Holistický přístup k řešení problému
- Výhoda multioborového zaměření členů týmu
- Těžení z reálných případů
- Jasná strategie



DECISION DOCUMENT

Geneva Cyber 9/12 Strategy Challenge

TEAM
Cybertarians

MEMBERS
Anna Blechová, Michaela Prucková, Jakub Vostoupal, Dominik Zachar

COACH
Jakub Drmola

TARGETTED ATTACK (PRIMARILY AT NISTRIA)

ALTERNATIVE SCENARIOS

Political responses	Societal responses	Medical responses	Technological responses	EU as a target
Responses aimed at political and diplomatic aspects, international relations and crisis management.	Responses with consequences to society.	Responses aimed at preserve the continuity of medical services.	Responses aimed at data analysis, CIA triad and redundancy mechanisms.	Nistria was exploited as the newest and weakest link.
<ul style="list-style-type: none"> ✓ NATO engagement and help ✓ Blueprint on coordinate response to large-scale cybersecurity incidents and crisis ✓ Reaching out to Mustelus to fight the cyberthreats ✓ Solving the situation with the leak of information 	<ul style="list-style-type: none"> ✓ Avoid the spread of panic ✓ Engaging media in the mitigation ✓ Monitoring the media and social media ✓ Intelligence gathering on social media accounts ✓ Engagement of civil society ✓ Restrictions on public gathering 	<ul style="list-style-type: none"> ✓ Triage system ✓ Clusters of cooperating medical services ✓ Do not shut down DigiSantEU ✓ Army involvement – field hospitals, transportation of patients, logistics etc. ✓ Involvement of private practitioners and clinics 	<ul style="list-style-type: none"> ✓ Data analysis – breach of CIA triad ✓ Sample testing ✓ Employment of redundancy mechanism ✓ Private sector involvement 	<p>Exploited installation error</p> <p>Faulty installation later used to infect other systems.</p>

DECISION DOCUMENT

Geneva Cyber 9/12 Strategy Challenge

MUNI

TEAM
NUKE them Cybertarians!

Legend

- Cyber-mandated operations
- Joint operations with other entities

TIMELINE	Stage 1 Immediate responses	Stage 2 Intermediate responses	Stage 3 Escalation responses
Passive policy option	<ul style="list-style-type: none"> ○ Isolate and clean affected systems ○ Disconnect from the satellites network 	<ul style="list-style-type: none"> ○ Stay offline ● Rescue the miners without cyber means 	<ul style="list-style-type: none"> ○ Engage law enforcement ● Declare state of emergency
Reactive policy option	<ul style="list-style-type: none"> ○ Re-establish situational awareness in the region ○ Involve CERT and Digital Forensics and Incident Response team ● Launch StratCom and engage stakeholders 	<ul style="list-style-type: none"> ● Downgrade military equipment ○ Pay Miraba with interest-free loan from the African Union ○ Launch Bug Bounty program ● Deploy security forces in the Nalpine region ● Launch CIMIC ● Limit the cash withdrawals 	<ul style="list-style-type: none"> ○ Constantly monitor the situation ○ Involve pan-African CERT ○ Continue to isolate and restore compromised systems ○ Apply Diplomatic Toolbox - sanctions ○ Coordinate response on the African Union level ● Deploy cyber units and electronic warfare preparations
Aggressive policy option	<ul style="list-style-type: none"> ● Declare state of peril to the country ○ Isolate affected systems ● Prepare capacity for offensive measures and electronic warfare 	<ul style="list-style-type: none"> ○ Apply Diplomatic Toolbox - sanctions ● Hack-back ● Deploy national guard ○ Ensure OPSEC 	<ul style="list-style-type: none"> ● Conduct destructive multi-domain operations

JAK VYPADALA OSTATNÍ ŘEŠENÍ?





Cyber Incident: Ras Abu Desalination Plant

Where Doha, Qatar



When November 21, 2022

What

- Short-term water supply disruptions inciting brief panic in local populace
- Displays at plant listed names of migrant worker known to have died
- Water supply nominal after a few days

How

- Alleged exploits (as assessed by Chinese IRC)
- STANDINGPALM – backdoor inserted via update in Yuma software used at desalination plants, attributed to USG by Chinese IRC
- ROCKSHOT – caused malfunction in temperature control sensors

Who

- Unassessed based on current reporting, uncertainties and intelligence gaps
- Chinese IRC attributed STANDINGPALM to USG
- Private researcher attributed ROCKSHOT to UAE

Assessment

Currently multiple critical uncertainties and intelligence gaps; reliance on uncorroborated third-party claims and analysis; STANDINGPALM and ROCKSHOT not definitively known to originate from same threat source or to operate as package

Risks to CNI

Reactions of allies

Chinese role in Qatar

Other actors

Implications and Considerations

NSC Strategic Objectives

Decrease uncertainty, know the risks

Demonstrate U.S. as a responsible cyber actor

Limit China's ability to exploit situation

Understand



1. USCYBERCOM and CIA to conduct internal review of cyber operations to understand origin of STANDINGPALM and extent of any possible USG utilization of it
By December 11
2. DNI to analyze and assess perpetrator of Ras Abu Fontas cyber incident and origin of ROCKSHOT malware and to develop options for public attribution based on level of confidence and classification of supporting intelligence
By December 14

Prepare



3. CISA and EPA, with support from relevant private sector coordinating councils, to conduct domestic vulnerability assessment of Yuma software and specific ICS exploits and, where relevant, provide prioritized remediation strategy – to be supported by general information campaign, promoted by EPA (e.g. “desalinate the network”)
By end December

Reassure



4. With FBI in lead via UAE LEGAT relationships, CISA to publicly offer technical support to Qatar to collect technical evidence and assist with remediation, while simultaneously requesting Fenghuang Labs to publicly share evidence used for analysis
By December 15
5. USG to use non-public classified military and diplomatic channels to reassure FVEY and NATO allies regarding its alleged involvement in incident and will share information when available
Ongoing



TO: National Security Council
FROM: Ghost in the Shellcode [W. DeSombre, M. Lee, E. Plankey, B. Saunders]
RE: Policy Options – Downstream Effects from Cyber Attack on Qatari Water Treatment Facility

EXECUTIVE SUMMARY: A cyber attack on a Qatari water treatment plant through compromising Yuma software led to minor disruptions and mass panic during the 2022 World Cup in Doha. This compromise may **impact U.S. industrial control systems**. A Chinese firm attributed the attack to the United States without sharing evidence. This **increased U.S. diplomatic tensions with France and Qatar**.

PRIMARY ASSESSMENTS:

Short-term Diplomatic Tensions [Severity: **High** | Likelihood: **High**]

- **We do not have U.S. intelligence confirming Chinese analysis.** Tensions with France and Qatar can increase risks to the Qatar USCENTCOM air base / U.S.-French counter cybercrime partnership.

Long-term ICS Cyber Defense [Severity: **Medium** | Likelihood: **Medium**]

- **We do not know how many U.S.-based desalination / water treatment plants use Yuma software.** If U.S. infrastructure is compromised, mass panic will likely also play a role.

RECOMMENDATION: COA2 – Aid and Attribution Diplomacy

COA2 provides solutions for domestic resiliency, concrete steps to engage France and Qatar, and mitigates diplomatic spillover of allegations against the U.S.

POLICY OPTIONS		
<p>COA1 - BASELINE <i>Full Transparency</i></p> <ul style="list-style-type: none"> □ CISA, USCERT, and WaterISAC identify U.S. vulnerabilities. □ FBI/NCIJTF publicly offer to support Qatar. □ State issues advisory on the World Cup. □ State issues a statement on protecting world cultural events. <p>□ Shows U.S. support on finding true perpetrators, proactively protects U.S.</p> <p>✗ Does not address U.S. attribution, limited engagement with private sector.</p>	<p>COA2 - RECOMMENDED <i>Aid & Attribution Diplomacy</i></p> <p>COA1 and:</p> <ul style="list-style-type: none"> □ State & FBI jointly state that USG is using all available sources to investigate. □ USIC conducts private attribution of actors. □ FBI reaches out to OCLCTIC to assist investigation, engages U.S. private sector partners. □ USAID offers to ship bottled water stockpiles to regions not connected to Qatari reserves. <p>□ Smooths tensions with France and Qatar.</p> <p>✗ Increases potential tensions with the Chinese government.</p>	<p>COA3 - AGGRESSIVE <i>Prepare Defenses</i></p> <p>COA2 and:</p> <ul style="list-style-type: none"> □ Public denouncement of U.S. attribution by U.S. Press Secretary. □ DOD notifies Al Udeid Air Base to be on alert for retaliatory, anti-U.S. protests. □ DOD offers to send an aircraft carrier to purify water in the Persian Gulf. <p>□ Ensures safety of USPERs in Qatar, preempts criticism of insufficient response.</p> <p>✗ Risks perception of acting disproportionately and antagonizes China, Qatar, and Iran.</p>

VÝSLEDKY

- 2021 – 10. místo (31)
- 2022 – 13. místo (34)



Universiteit
Leiden




Stockholm
University



LESSONS LEARNED

- Práce s nejistotou
- Nuke them je relevantní možnost řešení, přestože se může zdát absurdní
- Je důležité, jaká slova a rétoriku používáme
- Na porotě záleží, co se líbí jedné, naštve druhou
- Time management (je dobré počítat s možností, že tým postoupí)
- Delegace úkolů
- Důležitost kouče a jeho zkušeností
- Je třeba dobré zázemí





**DĚKUJEME ZA
POZORNOST**