The energy reserves in the Eastern Mediterranean Sea and a malicious campaign of APT10 against Turkey

lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/

Energy reserves in the Eastern Mediterranean Sea and the “MEDEAST” gas pipeline:

The Mediterranean Sea has become an increasingly relevant geostrategic topic for the Ministries of Foreign Affairs of Turkey, Greece, Cyprus, Israel and even China due to the controversies generated during the last decade for the discoveries of natural gas resources located in the Eastern Mediterranean seas of States such Israel, Cyprus and Egypt ([1]).

The presence of Turkish troops in Libya and Syria, and the Franco-Greek alliance to avoid Turkish intrusions in the maritime territory of Greece show the relevance and global interest in energy resources in the area.

As it could be seen in the following map, part of the geostrategic conflict is focused on the Turkish EEZ. Turkey carried out an agreement with Libya which tries to carry out an expansion of its exclusive maritime economic zones ([2]).

It is relevant to clarify that an EEZ is a maritime zone prescribed by the United Nations Convention on the law of the sea over which a state has special rights regarding the exploration and exploitation of sea resources, including the production of energy through the water and wind ([3]) ([17]):

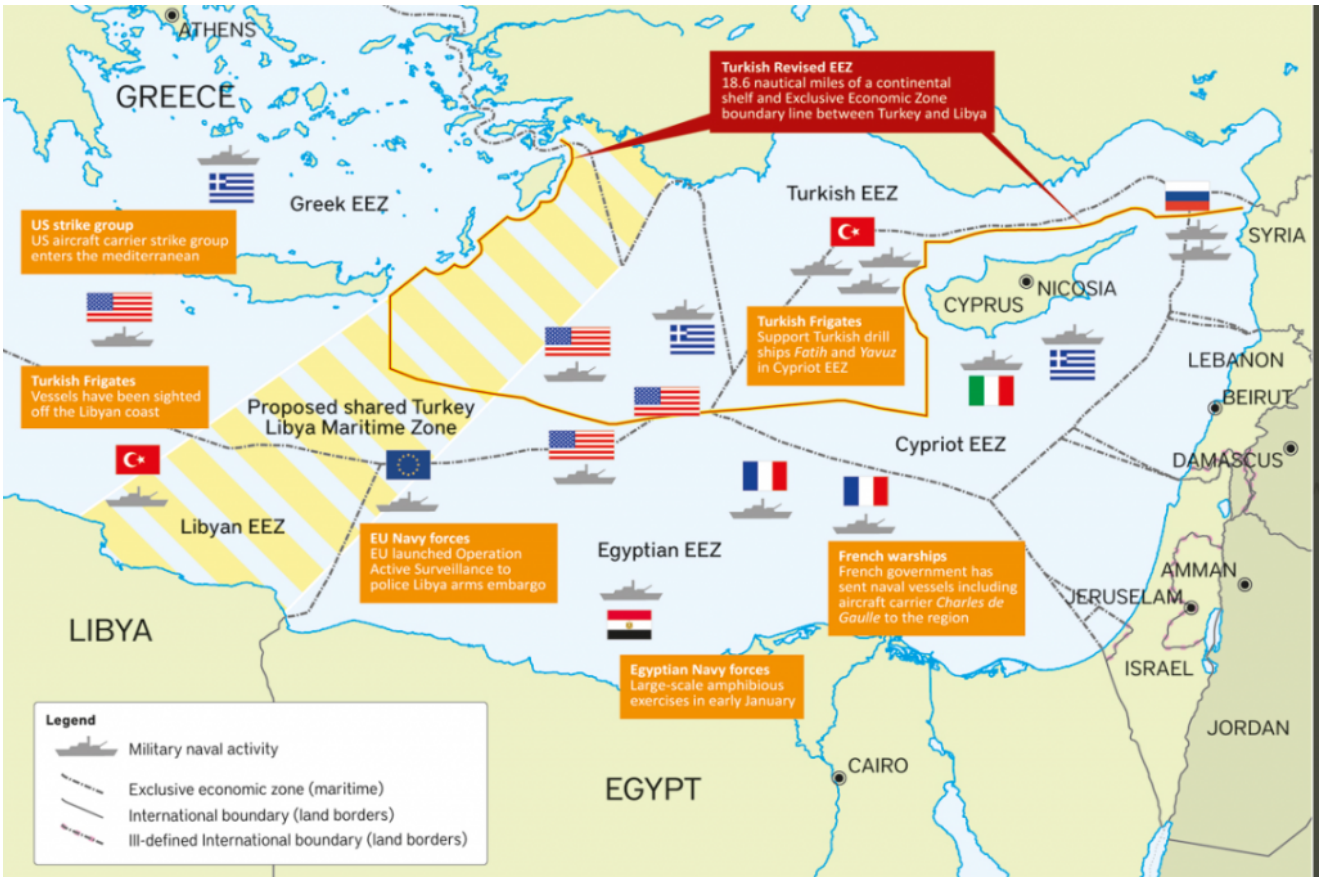

Illustration 1. Expansion of Turkish EEZ

The expansion that the Turkish government tries to carry out could increase the geopolitical risk among Cypriots, Greeks and even Israeli governments. The military presence in the area by those States could be seen in the map shown above. The strategy of increasing Turkey's EEZ would leave without an important part of the continental shelf Athens ([4]). In addition, Cyprus is significantly affected by this EEZ's expansion as there is an occupation of the Cyprus' EEZ area. Furthermore, the President Erdogan has publicly declared that his oil exploration projects in the coast of Cyprus will not cease. Turkey tries to stablish a zone of EEZ controlled by the Turkish influence which would be represented as in the following map ([5]):

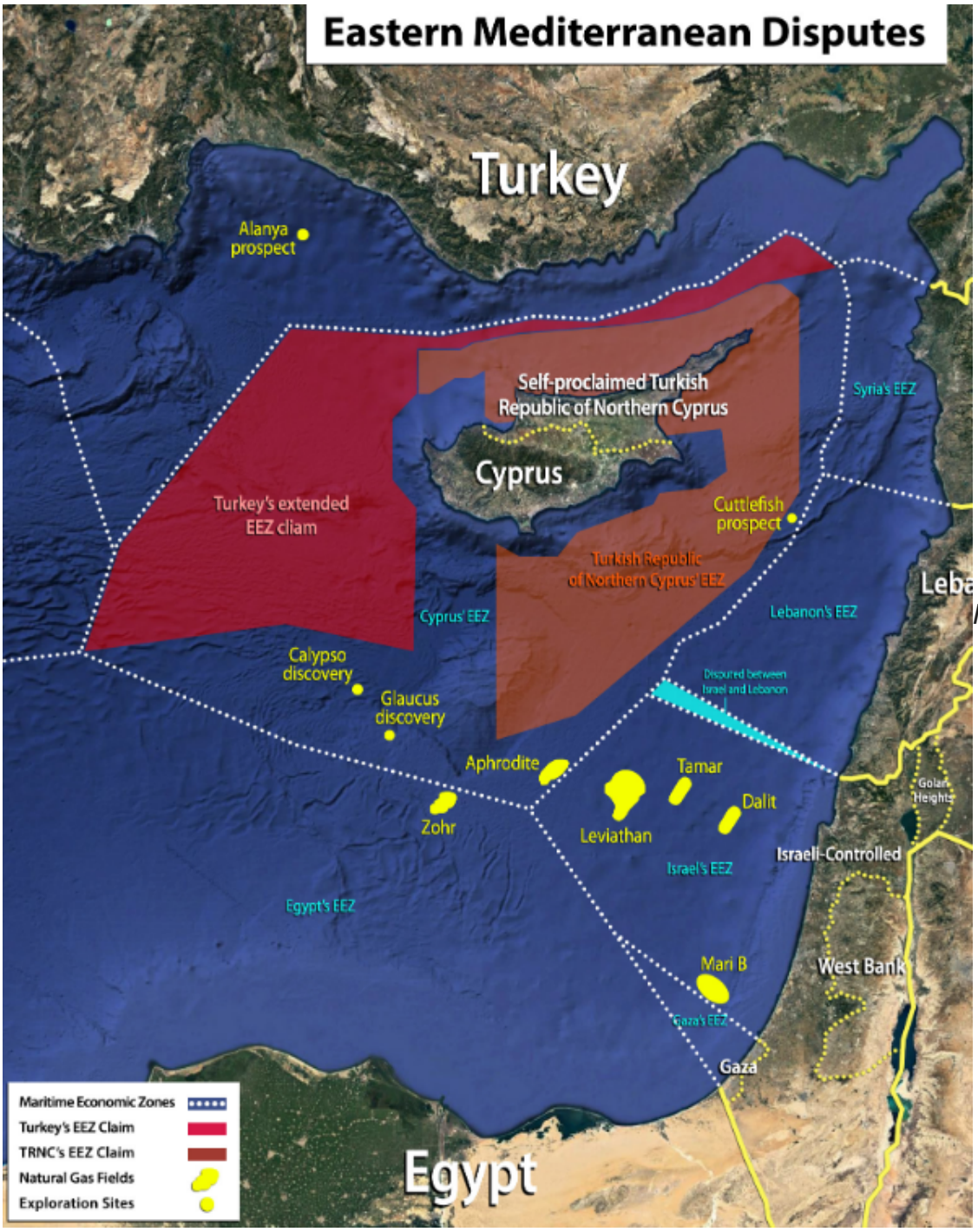

Illustration 2. Expansion of the Turkish EEZ and location of energy resources

In the previous map, you can see which energy exploration areas are located in Israel, Cyprus and Egypt. Moreover, these States give diplomatic support to Cyprus and Greece regarding the expansion's conflict of the Turkish EEZ.

Furthermore, the 27th of February of 2020, Greece, Cyprus and Israel signed an agreement to build up a gas pipeline to transport gas to Europe from the Leviathan gas reserves located in Israel. Moreover, in the near future there is the intention of joining to the pipeline the extractions from the Cypriot gas reserves, Aphrodite and Calypso ([6]).

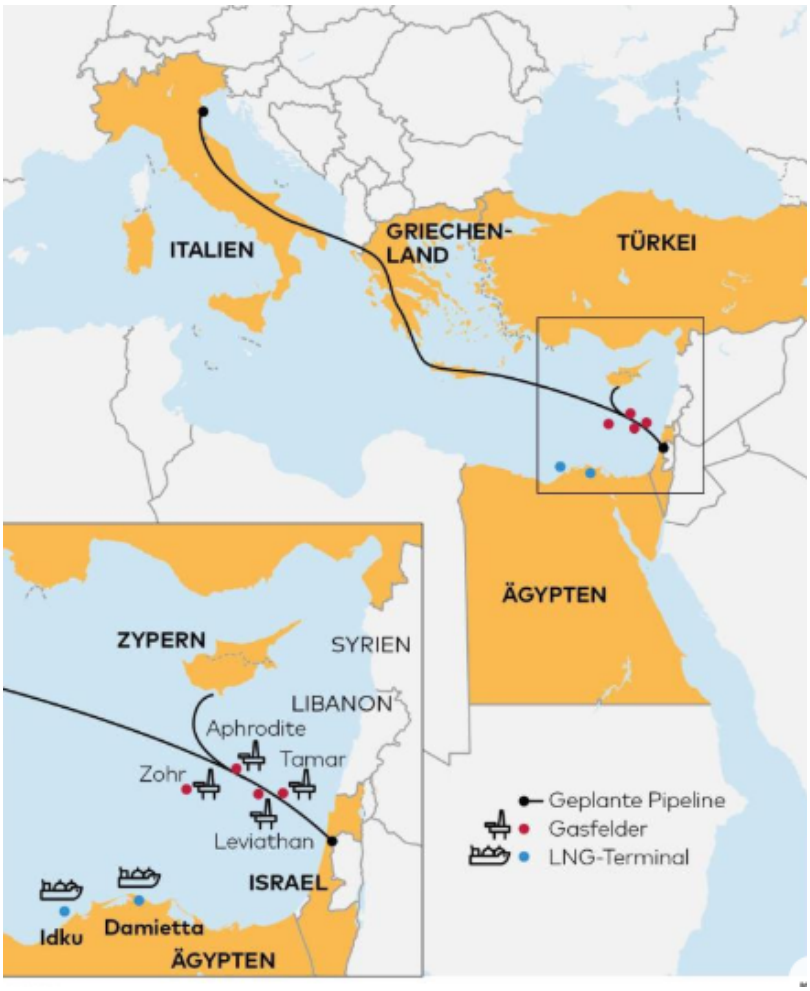

Illustration 3. Mediterranean Gas Pipeline

Turkey has displaced several warships to the coast of Cyprus in order to carry out gas exploration projects. The Eastern European gas pipeline reduces the geopolitical power of Turkey as it tries to exclude Turkey from any participation in it. This “pipeline” has been called “EastMed” ([6]). However, during March, Turkey will put an offshore drilling vessel in order to continue with its oil exploration projects in the EEZ waters of Greece, Cyprus and the EU in order to try to acquire in the future the role of gas supplier for the EU ([8]).

Interests and influence of China in the Mediterranean area:

China, unlike the US diplomatic-military expansionism, has focused its expansionist strategy on the diplomatic-commercial strategy. For China, one of its geo-strategically key regions, has been the Port of Piraeus of Greece. The Greek government tendered for the next 35 years the 67% of the Port’s operations to COSCO (China Ocean Shipping Company) for 368.5 million and 350 million of euros to be invested in the Piraeus’ port infrastructure ([9]).

The Port of Piraeus represents a potential gate of all the commercial flow that comes from the OBOR sea route. In addition, during November of 2019, China and Greece signed up 16 cooperation agreements of different matters, including trade and energy investments ([10]).

On the other hand, Cyprus signed an agreement with a consortium led by China to build up the first natural gas import terminal in Cyprus. The terminal is designed to convert imported liquefied gas into a gaseous form to be used in energy plants ([11]). The construction is being developed by China Petroleum Pipeline Engineering, Metron, Hudong-Zhngua Shipbuilding and Wilhelmsen Ship Management. Construction is expected to be done in 2022.

Regarding the international security, China investigates Turkey's relation with the Uighur community. The Uyghurs are Turkish-speaking people from the interior of Asia and mostly of them have Muslim religious confession. The Uyghurs live in northwestern China, in the Uyghur autonomous region of Xinjiang and are considered a threat to the People's Republic of China as they are considered largely jihadist terrorists ([12]).

Turkey is the country that has given the most international support to the Uyghur community. Currently, up to 45,000 Uyghur refugees live in Turkey on a temporary visa or even with a permanent residence permit ([13]).

Turkey's foreign affairs policies are misaligned from those of China. The possible obstruction of the OBOR route to the Port of Piraeus and the collaborative policies with the Uyghur community in the Xinjiang region of China could damage their diplomatic relations.

Due to the diplomatic confrontations and conflicting interests of the two countries, China could carry out cyber espionage operations against Turkish organizations and institutions linked to diplomacy, defense, energy, telecommunications and foreign trade. Its main objective could be to collect confidential information in order to gain advantages within the future geostrategic movements of Turkey and the rest of the actors involved in the conflicts over the energy resources located in the Mediterranean Sea.

Malicious campaign against Turkish organizations:

A malicious campaign allegedly attributed to APT10 against Turkish organizations from various sectors such as telecommunications and finance has been identified by Adeo in January of 2020 ([14]). APT10 is a group presumably attributed to the Ministry of State Security of China ([15]). In addition, it is a group that usually targets organizations from various sectors such as defense, energy, health, telecommunications, governments, military, shipping and IT ([16]).

It has been identified that APT10 usually carries out malicious campaigns against organizations that could damage the China's State interests into the global market. On the other hand, it has also been detected that APT10 usually carries out malicious campaigns against organizations that support foundations which carry out aid projects with ethnic groups that may be a potential threat against the Chinese national security, as the case of the Uyghur community.

Moreover, in this campaign has been identified several similarities with the TTP published in other APT10 reports in 2019 ([14]). In this case, it was identified that this campaign began in 2016 and the initial access was carried out with the exploitation of a public web application.

Summary of the executed Kill Chain ([14]):

• Initial access:

The attackers deployed the following China Chopper4, JspSpy5 webshells to obtain a foothold on the victim's network that they used to execute commands to upload files to the target machines.

• Reconnaissance, execution and theft of credentials:

In the reconnaissance phase, a series of commands were launched to collect information from users, domains and shared folders. The hostile actor used legitimate tools of the Windows operating systems for the reconnaissance stage, such as "ipconfig.exe", "whoami.exe", "net.exe", "ping.exe", "powershell.exe" and " BloodHound "(bloodHound is not a legitimate binary from Microsoft). The attacker used an advanced tool called "dns.exe" to list all the machines that were registered in a particular domain.

Regarding the execution, the hostile actor implemented "hTran" backdoor to be able to exfiltrate information. In previous malicious APT10 campaigns against Turkey, this executable file was seen with the name "java.exe" on compromised hosts.

Hostile actors loaded a malicious DLL into the memory of a legitimate binary. The final payload is injected into the legitimate process "svchost.exe". It was identified that this payload was a PlugX variant or a CobaltStrike Beacon as a post-exploitation framework.

To carry out the theft of credentials the hostile actor used the following tools: "QuarksPWdump" and "Mimikatz".

• Lateral movements

Through the lateral movements they were able to compromise critical servers and gain access as a domain administrator. The group used NTLM hashes to move laterally. They used the tools "net.exe", "wmic.exe", "psexec.exe", "smbexec", and "wmiexec".

• Persistence

The advanced group established persistence in certain servers that were of their interest and deployed a remote access Trojans such as "QuasarRAT" and "PlugX", moreover penetration or "pentesting" tools such as "Cobalt Strike" and "kerberos".

• C&C connections

Hostile actors used two different ways to keep connections with C&C servers. Once the vulnerability was exploited to establish itself on the public server, the group moved to the “terminal server”. To establish communications with the other hosts in the internal network, they installed an SMB beacon on the “terminal server”, using it as a bridge between the internal network and the C&C server.

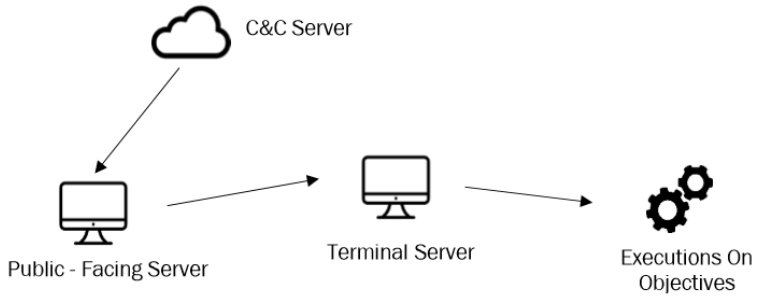

Illustration 4. First C&C communication

method

However, the group established a different method for hosts that had direct access or had a proxy. In this case they used the http protocol to establish the communications with the C&C.

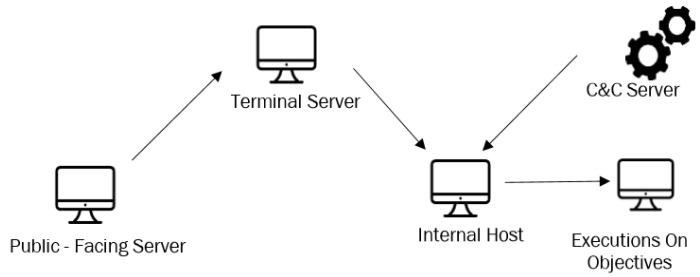

Illustration 5. Second C&C communication

method

In the following chart, there are the TTPs developed by APT10 during this malicious campaign against the Turkish organizations ([16]) ([14]):

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Access Token Manipulation	Access Token Manipulation
	Execution through Module Load	Create Account	DLL Search Order Hijacking	Connection Proxy
	PowerShell	DLL Search Order Hijacking	Exploitation for Privilege Escalation	DLL Search Order Hijacking
	Scheduled Task	New Service	New Service	DLL Side-Loading
	Scripting	Scheduled Task	Scheduled Task	File Deletion
	Service Execution	Web Shell	Web Shell	Masquerading
	Windows Management Instrumentation	Windows Management Instrumentation Event Subscription		Modify Registry
				Network Share Connection Removal
				Scripting

Credential Access	Discovery	Lateral Movement	Collection	Command And Control
Account Manipulation	Account Discovery	Pass the Hash	Automated Collection	Commonly Used Port
Credential Dumping	Browser Bookmark Discovery	Pass the Ticket	Data from Local System	Connection Proxy
Credentials from Web Browsers	Network Share Discovery	Remote Desktop Protocol		Remote Access Tools
Steal Web Session Cookie	Process Discovery	Remote File Copy		Remote File Copy
		Windows Admin Shares		

Exfiltration
Data Compressed
Data Encrypted

Illustration 6. TTP used in the APT10 campaign

Recommendations:

It is recommendable that the organizations from the defense sector, governments, energy, telecommunications and finance linked to projects that may affect the interests of China apply the maximum prevention to this increase of malicious campaigns from APT groups presumably linked to China.

It is recommended to apply the IOC of the APT identified as a threat by their intelligence provider LAB52 as soon as possible.

It is recommended to keep the operating systems, services and tools used in the organization updated with the latest security patches.

It is recommended to establish security policies (GPOs) to control accesses and actions carried out in those systems and / or services that are exposed to the internet.

Conclusions:

Since the last decade, Turkey has acquired an important influence in the energy geopolitics of the Eastern Mediterranean Sea. The Turkish foreign policies has hindered the China's international trade strategies. Furthermore, the diplomatic Turkish support to certain Chinese ethnic groups that are considerate as a threat against the Chinese national security, could

provoke that Turkey becomes a target of groups like APT10 which presumably are linked to the Ministry of State Security of China. APT10 is a group that has a wide range of targets. The organizations from sectors of interest for the government of China and the organizations that have some kind of link with the commercial development of the OBOR route could be susceptible to being targeted by groups such as APT10.

References:

[1] https://www.mei.edu/publications/turkeys-eastern-mediterranean-quagmire

[2] https://www.petroleum-economist.com/

[3] https://greece.greekreporter.com/2018/10/12/greece-egypt-aim-to-strangulate-turkey-in-east-med-turkish-daily-claims/

[4] https://moderndiplomacy.eu/2019/12/20/the-exclusive-economic-zone-between-libya-and-turkey/

[5] https://www.ozelburoistihbarat.com/kitalar-bolgeler-akdeniz-karadeniz-ege-marmara/dogu-akdenizde-tartisma-harita-uydu-goruntuleri-eren-talha-altun-12708

[6] Kontakos P. (2018) Blue economy enterpreneurship in Offshore Energy in Cyprus and Greece. Journal of International Scientific Publications

[7] https://www.welt.de/wirtschaft/article204725766/EastMed-Das-ist-Europas-neue-Problem-Pipeline.html

[8] https://www.turkishminute.com/2020/02/19/turkey-buys-third-drilling-ship-for-mediterranean-gas-exploration-erdogan/

[9]https://www.cidob.org/en/publications/publication_series/notes_internacionals/n1_156/china_moors_in_the_mediterranean_a_sea_of_opportunities_for_europe

[10] https://www.aljazeera.com/news/2019/11/greece-china-hail-strategic-partnership-eu-191111170150762.html

[11] http://www.ekathimerini.com/247559/article/ekathimerini/news/chinese-led-consortium-to-build-cyprus-gas-import-terminal

[12] https://www.icij.org/investigations/china-cables/china-cables-who-are-the-uighurs-and-why-mass-detention/

[13] https://www.voanews.com/extremism-watch/uighurs-concerned-china-luring-turkey-silence-xinjiang

[14] Adeo IT Consulting Services. January 2020. APT10 Threat Analysis Report. https://adeo.com.tr/en/adeo_annual_threat_report/

[15] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[16] https://attack.mitre.org/

[17] https://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm