Thomas Murray

Middle East Conflict: Risk Briefing

March 2026

17 March 2026

Welcome

Jim Micklethwaite | Head of Financial Markets
jmicklethwaite@thomasmurray.com

Today’s Agenda

01 Introduction

02 Conflict Overview

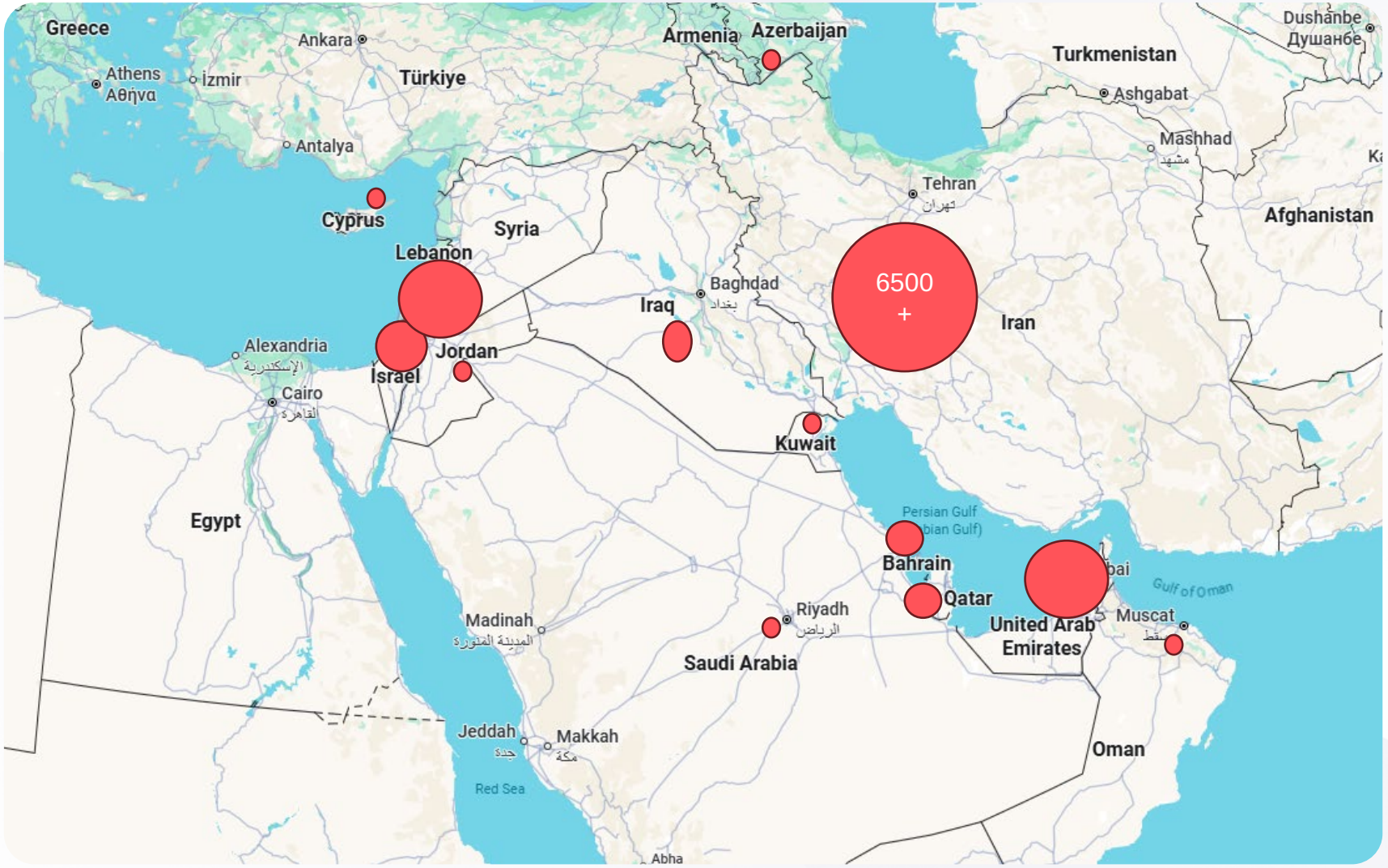
03 Banking and Financial Services Impact

04 Cyber Threat Intelligence

Thomas Murray

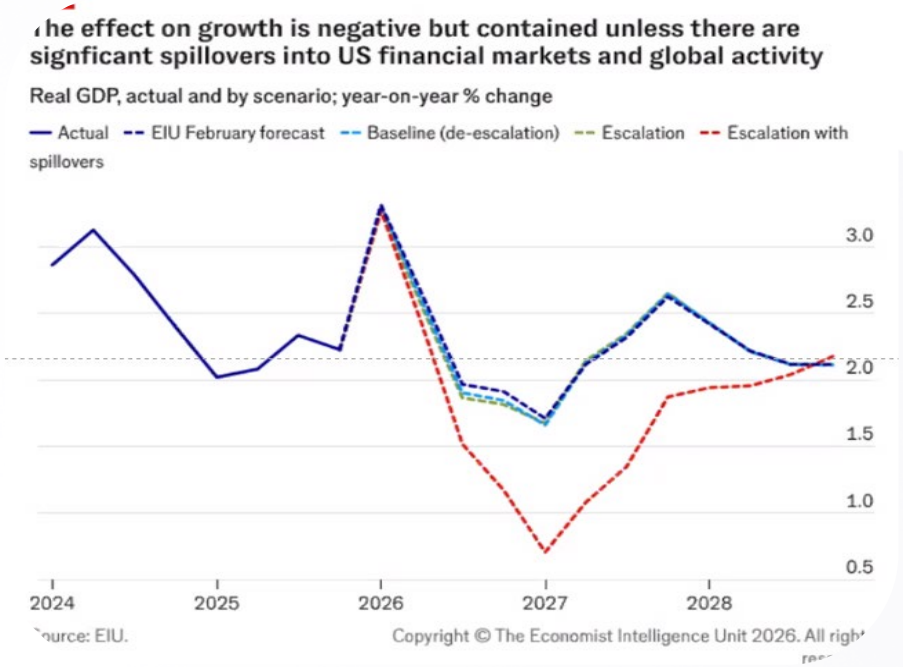
Conflict Overview

Strike volume over 18 days

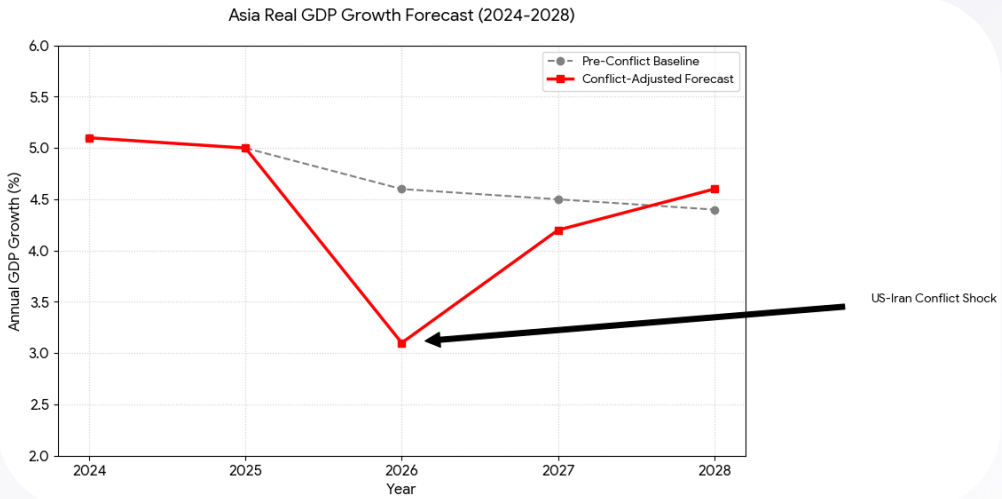


Economic Impact

US

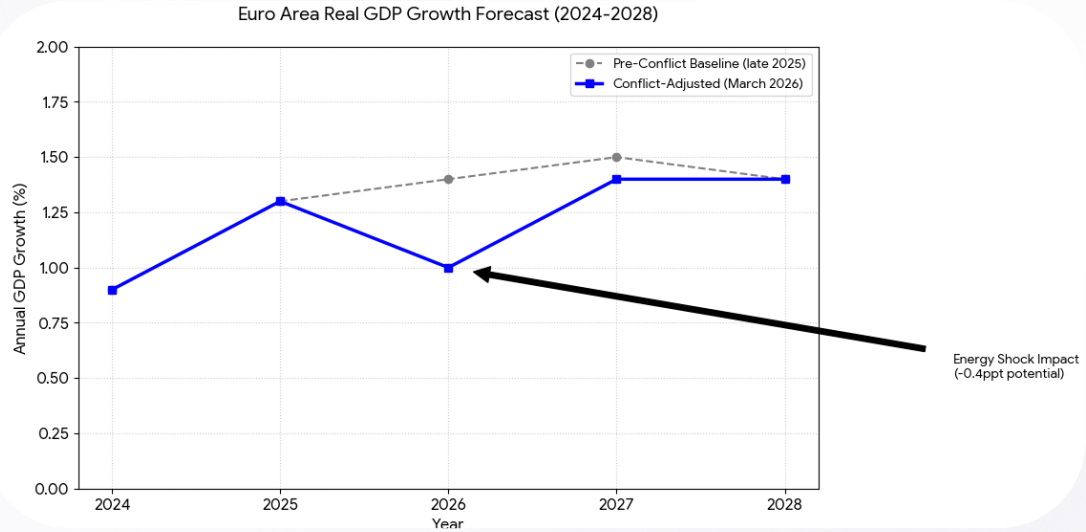


Asia



Source: Asian Development Bank.

EU



Source: Oxford Economics & Goldman Sachs.

Banking and Financial Services

Stacey Fernandes | Senior Analyst - Financial Market Infrastructure
sfernandes@thomasmurray.com

Middle East Markets Impacted – FMIs and Banks

Bahrain, Egypt, Israel, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, Turkey, UAE

FMI's

- Bahrain Clear - BCP activated with 70% staff working remotely.
- Midclear activated BCP with staff working from its DR, on-site and remotely.
- Kuwait CSD - Hybrid working model implemented with 70% staff working remotely.
- Qatar CSD (Edaa) - BCP activated with non-critical staff working remotely.
- Turkey - Precautionary measures announced by the CMB and the central bank.
- UAE: DFM, hybrid arrangement with 50% staff working remotely. ADX, liquidity measures in place.

Banks

- Central Bank of Bahrain affirms banking and financial sector operations.
- Central Bank of Kuwait confirmed all financial payment systems in the country are working normally.
- Qatar Central Bank issued a mandatory remote-work directive for all financial institutions.
- The CBUAE confirms financial sector remain stable and fully operational.
- Several major banks have altered their physical presence with the safety of staff prioritised.

Middle East Markets Impacted – FMIs and Banks

Bahrain, Egypt, Israel, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, Turkey, UAE

- The Thomas Murray Risk Committee reviewed and revised downwards the Country Risk score in the Market Asset Safety Risk Assessment (MASRA). Changes to the country risk score did not result in any changes to the overall grade of the affected markets.

Country	Old Score	Revised Score	Overall Grade (No Change)	Overall CSD Risk Grade
Bahrain	4.61	3.61	A-	Bahrain Clear: A-
Egypt	2.53	2.28	A-	MCDR: A+ ECSD: A+
Israel	5.18	4.18	A	TASECH: A+
Jordan	5.55	5.3	A	SDC: A+
Kuwait	6.31	5.31	A	KCSD: A-
Lebanon	2.28	1.28	BB	Midclear: A- CBL: BBB
Oman	6.65	6.2	A+	MCD: A
Qatar	6.95	5.95	A	Edaa (QCSD): A-
Saudi Arabia	5.79	4.49	A+	Edaa: A+
Turkey	2.38	2.13	BBB	MKK: A+ CBT: A
UAE	7.44	6.65	A+	AD CSD: A- Dubai CSD: A Nasdaq Dubai: A
USA	7.48	6.98	A+	DTC: AA Federal Reserve: AA

- Both the Overall Risk Outlook and the Operational Risk Outlook for the Middle-East CSD's and sub-custodian banks affected, continue to remain on "On-Watch".

Cyber Threat Intelligence

James Thoburn | Director, Incident Response
jthoburn@thomasmurray.com

Cyber is now a part of the battlefield in the Middle Eastern conflict

A Recap

- **Petrol station payment systems disrupted in Jordan**
  Handala group claims shut-down of all "gas" stations
- **US and Israeli military provider networks targeted**
  Increased data destruction and threat activity operations conducted against targets
- **Over 100 pro-Iranian Hacktivist groups mobilised**
  Building on Iran's long history of enabling Hacktivist groups
- **Previously compromised industrial control systems a concern**
  Given potentially long dwell times and change cycles, previously compromised systems may still be an issue
- **Retaliation against psychological operations expected**
  At the outset of the war an Iranian prayer app was used to send messages suggesting surrender. Iran is equally skilled in psychological operations

In the last week....

Handala's new destructive playbook

1. The group hijacked Microsoft intune to launch a global wipe attack on 200k+ devices in 79 countries.
2. The group is now actively targeting payment infrastructure (e.g. Verifone)
3. They are also targeting senior Israeli Intelligence figures and naval personnel
4. This signals a shift from espionage to large-scale data-destruction and psychological ops.

Hacktivist coalition surge & Russian alignment

1. The Iranian Electronic Operations Room now coordinates > 60 active groups
2. Pro-Russian actors have merged under the #OpIsrael banner
3. Massive DDoS bursts against banks, government portals and critical-infrastructure across the GCC and the U.S

Cyber-kinetic interplay via CCTV/IP-camera exploits

1. A spike in exploitation of Hikvision/Dahua cameras is being used for pre-strike target confirmation and post-strike battle-damage assessment, making camera compromise an early indicator of imminent kinetic action

Recent Operations

Summary of key attacks from February 2026 as a result of the ongoing conflict.

Date	Target / Operation	Detail
Pre-Feb 2026	**Israeli CNI / energy**	Claimed compromise of Israeli energy exploration company, oil and gas sector, Jerusalem CCTV streams, Israeli military weather servers
Pre-Feb 2026	**Jordan fuel systems**	Claimed compromise of Jordan fuel distribution infrastructure, claimed access to system controls
Pre-Feb 2026	**Israeli healthcare**	Targeted Israeli civilian healthcare infrastructure ahead of kinetic conflict to create domestic pressure
11 Mar 2026	**Stryker Corporation**	Wiper attack via Microsoft Intune abuse; 200,000+ devices wiped across 79 countries; 50TB claimed exfiltrated; SEC 8-K filed same day
11 Mar 2026	**Verifone**	Claimed breach of payment solutions provider; widespread disruption to payment systems and terminals; financial transaction data extracted
14 Mar 2026	**Israeli Navy**	Doxxing of 50 senior naval officers: names, photographs, ranks, home addresses, personal phone numbers published publicly on handala-redwanted.to
15 Mar 2026	**Mossad / INSS (Gilinski)**	Claimed 100,000 emails from former Mossad Deputy Head; hack-and-leak psychological operation targeting senior intelligence figure

Thomas Murray

Threat Assessment

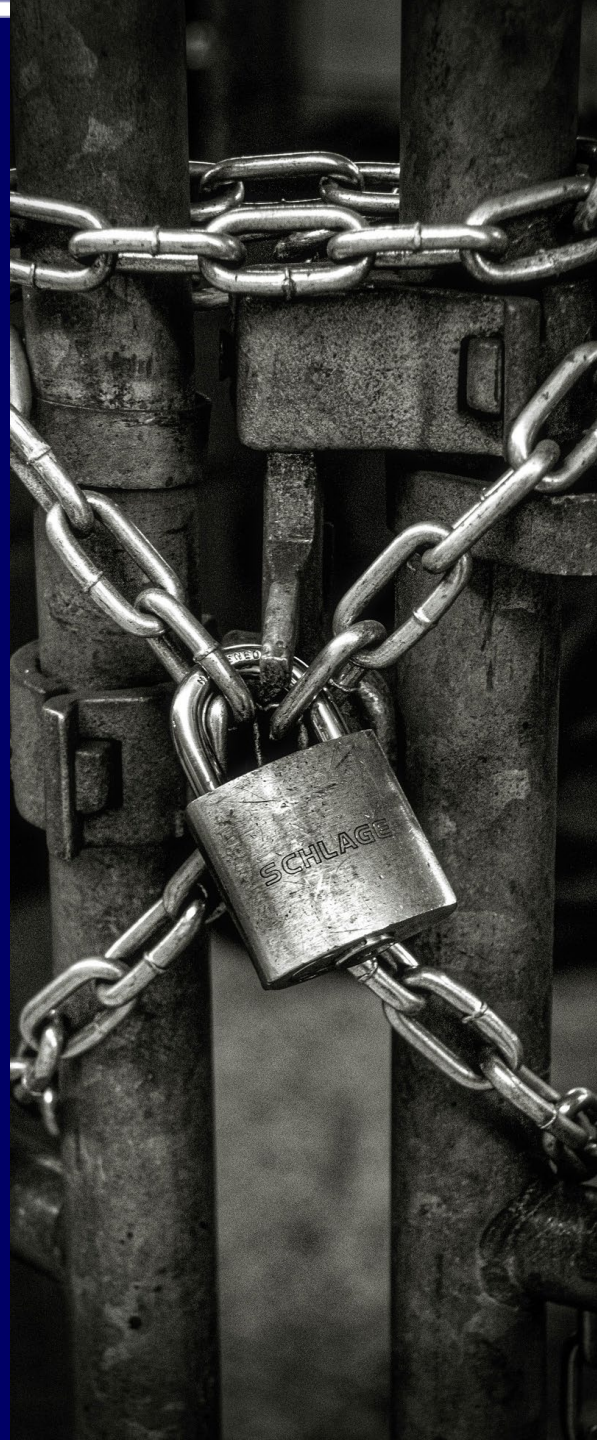
Country	Threat
Israel	CRITICAL
UAE	HIGH
Jordan	HIGH
Kuwait	HIGH
Bahrain	HIGH
Saudi Arabia	HIGH
Qatar	HIGH
Oman	MEDIUM

Sector	Threat
Financial Services	CRITICAL
Critical Infrastructure	CRITICAL
Transport and Shipping	HIGH
Government and Defence	CRITICAL
Media and Communications	HIGH
Hospitality and Tourism	MEDIUM

Thomas Murray

Security Advice

1. Assess assumption of compromise
2. Assess supply chain and dependencies
3. Know your assets, patch and secure them
4. Take immutable backups, ideally offline
5. Be ready to activate denial of service mitigation
6. Restrict/monitor traffic from affected geographies
7. Separate and monitor OT/ICS. Check for anomalous behaviour
8. Monitor CCTV/Security assets for vulnerabilities or insecure configurations
8. Monitor supplier access
9. Raise employee awareness and activate IR readiness
10. Ask for help if needed



Thomas Murray

Thomas Murray

Thank you

17 March 2026