Opérations israélo-américaines contre les programmes nucléaires au Moyen-Orient (1981- 2026)

Institut EGA

Bombardements, sabotages technologiques, cyberattaques et assassinats ciblés façonnent la lutte d'Israël contre la prolifération nucléaire au Proche et Moyen-Orient.

Depuis plus de quarante ans, Israël a mené une série d'opérations visant à neutraliser les programmes nucléaires perçus comme menaçants au Moyen-Orient. Ces actions combinent bombardements aériens, sabotages technologiques, cyberattaques et éliminations ciblées de scientifiques.

Les opérations emblématiques incluent la destruction du réacteur irakien d'Osirak en 1981, le bombardement du site syrien d'Al-Kibar en 2007, et les frappes contre les installations nucléaires iraniennes en 2025 et 2026. À chaque étape, Israël a mené les premières actions, parfois avec un soutien stratégique ou des frappes complémentaires des États-Unis.

Israël considère l'acquisition de l'arme nucléaire par ses adversaires régionaux, notamment la République islamique d'Iran, comme une menace existentielle. L'État hébreu a progressivement développé une stratégie mêlant frappes préventives, sabotages et opérations de renseignement.

Stratégies multiformes

Cette confrontation ne se limite pas aux raids aériens : des cyberattaques majeures comme *Stuxnet* et des assassinats ciblés, dont celui de Mohsen Fakhrizadeh en 2020, ont été intégrés à une « guerre à bas bruit » visant les infrastructures et les acteurs clés du programme nucléaire iranien.

Depuis 1981, la lutte contre la prolifération nucléaire s'est progressivement transformée en une stratégie hybride, mêlant moyens militaires, technologiques et clandestins pour contenir la menace régionale.

1981 – Irak : destruction du réacteur d'Osirak

Le premier bombardement

Le 7 juin 1981, l'aviation israélienne bombarde le réacteur nucléaire irakien d'Osirak dans le cadre de l'opération *Opera*. L'installation est encore en construction et Israël cherche à empêcher toute capacité irakienne de produire du plutonium à usage militaire.

L'opération est menée unilatéralement par Israël et provoque une forte réaction internationale, notamment une condamnation du Conseil de sécurité de l'ONU. Un an plus tôt, en 1980, le site avait déjà été visé par un raid iranien qui avait causé des dégâts limités avant sa remise en état.

2007 – Syrie : destruction du site d'Al-Kibar

2007, l'opération secrète

Le 6 septembre 2007, Israël bombarde un site situé près de Deir ez-Zor, dans l'est de la Syrie, lors de l'opération *Outside the Box*. L'installation est soupçonnée d'abriter un réacteur nucléaire clandestin construit avec l'aide de la Corée du Nord. L'attaque détruit entièrement le complexe. Ce bombardement a été revendiqué par Israël en 2018, onze après les faits.

L'opération est menée militairement par Israël seul, même si **les services de renseignement américains avaient identifié en amont la nature probable du site** et partagé leurs informations avec Tel-Aviv.

2025 – Iran : frappes contre le programme nucléaire

Le tournant de juin 2025

En juin 2025, dans le cadre de la « guerre des douze jours » entre Israël et l'Iran, plusieurs installations nucléaires iraniennes sont visées.

L'aviation israélienne mène les premières frappes contre des sites stratégiques du programme nucléaire. **Les États-Unis interviennent ensuite**, en coordination avec Israël, et frappent à leur tour plusieurs installations majeures, notamment Fordow, Ispahan et Natanz. Ces opérations s'inscrivent dans un conflit plus large comprenant également des frappes militaires et des opérations ciblées contre des responsables et scientifiques iraniens.

2026 – Iran : nouvelles frappes conjointes

La division opérationnelle américano-israélienne

Depuis la fin février 2026, de nouvelles attaques ont visé certaines installations nucléaires iraniennes, endommageant notamment des infrastructures d'accès.

Ces opérations sont présentées comme des **actions conjointes entre Israël et les États-Unis**, dans la continuité de l'escalade militaire initiée en juin 2025 mais avec un niveau de coordination inédit.

Washington concentre ses efforts sur les infrastructures nucléaires et atomiques, tandis que Tel-Aviv privilégie les centres de répression et certaines installations militaires. Cette approche duale cherche à éroder simultanément les deux piliers de la République islamique : sa capacité de dissuasion stratégique et son appareil de coercition interne.

UNE STRATÉGIE DE « GUERRE À BAS BRUIT »

→ À côté des frappes aériennes, la confrontation autour des programmes nucléaires s'est aussi déroulée dans l'ombre. Des **cyberattaques sophistiquées**, comme l'opération *Olympic Games* et le virus *Stuxnet*, ont saboté à distance des centrifugeuses utilisées pour l'enrichissement de l'uranium.

→ Parallèlement, plusieurs scientifiques et responsables du programme nucléaire iranien ont été assassinés lors d'opérations d'assassinats ciblées, dont le cas le plus emblématique reste celui de Mohsen Fakhrizadeh en 2020. D'autres physiciens et ingénieurs ont été tués entre 2010 et 2025.

Ces actions s'inscrivent dans une stratégie de « guerre à bas bruit », combinant **cyber-sabotage, opérations clandestines et frappes ciblées** pour ralentir ou désorganiser les programmes nucléaires sans déclencher immédiatement un conflit ouvert.

Cyberattaques et sabotages technologiques

***Stuxnet* (2009-2010)** : La plus célèbre cyberattaque reste *Stuxnet*, découverte en 2010 mais déployée probablement dès 2009 contre l'installation d'enrichissement de Natanz. Le malware ciblait les systèmes industriels Siemens contrôlant les centrifugeuses IR-1. En modifiant imperceptiblement leur vitesse de rotation, il aurait détruit environ 1 000 centrifugeuses et retardé le programme iranien de plusieurs années. L'opération est largement attribuée à une coopération entre les États-Unis et Israël (NSA et unité 8200).

***Duqu* (2011)** : Peu après *Stuxnet*, un malware nommé *Duqu* a été découvert. Il est considéré comme une sorte de « cousin » de *Stuxnet* : il ne sabotait pas directement les installations mais collectait des renseignements sur les systèmes industriels afin de préparer d'éventuelles attaques futures.

***Flame* (2012)** : Un autre logiciel espion extrêmement sophistiqué, *Flame*, a été découvert en 2012 et visait plusieurs pays du Moyen-Orient, notamment l'Iran. Il servait à surveiller des réseaux gouvernementaux et scientifiques, collecter des documents et enregistrer des communications.

Plus récemment, plusieurs cyberattaques ont perturbé des infrastructures civiles iraniennes (stations-service, systèmes ferroviaires, sites gouvernementaux). Certaines ont été revendiquées par des groupes se présentant comme hostiles au régime iranien et soupçonnés d'avoir des liens avec Israël. Elles ne visaient pas directement le nucléaire mais s'inscrivent dans la confrontation stratégique entre les deux États.

Pendant la guerre de juin 2025 et depuis fin février 2026, des opérations cyber ont accompagné les frappes militaires. Les services israéliens ont notamment :

- mené des opérations de cyber-espionnage contre des infrastructures militaires et stratégiques iraniennes
- perturbé certaines communications et systèmes de commandement.

Les cyberattaques majeures contre le nucléaire restent surtout 2010-2012 (Stuxnet, Duqu, Flame). **Les années récentes relèvent plutôt de cyber-appui militaire**.

Actions clandestines sur site

Explosion de Natanz (2020) : En juillet 2020, une explosion majeure a détruit un bâtiment du complexe nucléaire de Natanz, où étaient assemblées des centrifugeuses avancées. Les autorités iraniennes ont parlé de sabotage ; plusieurs médias occidentaux ont attribué l'opération au Mossad.

Sabotage électrique de Natanz (2021) : En avril 2021, une panne électrique massive a touché l'installation d'enrichissement de Natanz. L'Iran a accusé Israël d'avoir saboté le système électrique souterrain du site, endommageant de nombreuses centrifugeuses.

Assassinat de scientifiques nucléaires iraniens

Plusieurs assassinats ont eu lieu au début des années 2010, souvent par **bombes magnétiques fixées sur des voitures à Téhéran**.

Massoud Ali-Mohammadi (2010) : Physicien nucléaire tué par bombe télécommandée devant son domicile à Téhéran.

Majid Shahriari (2010) : Scientifique impliqué dans le programme nucléaire tué par bombe magnétique placée sur sa voiture.

Dariush Rezaeinejad (2011) : Ingénieur lié au programme nucléaire abattu devant son domicile.

Mostafa Ahmadi Roshan (2012) : Responsable à l'installation de Natanz, tué également par bombe magnétique sur son véhicule.

Mohsen Fakhrizadeh (2020) : Le cas le plus célèbre. Considéré comme l'architecte du programme nucléaire militaire iranien, il a été assassiné près de Téhéran dans une opération très sophistiquée attribuée au Mossad.

La situation change avec la guerre de juin 2025. Plusieurs scientifiques du programme nucléaire iranien ont été tués lors des frappes israéliennes, notamment :

- Ahmadreza Zolfaghari (professeur de physique nucléaire)
- Abdolhamid Minouchehr (physicien nucléaire et responsable académique)
- Ali Bakouei (scientifique impliqué dans le programme nucléaire iranien)
- Akbar Motalebizadeh (ingénieur nucléaire universitaire)
- Issar Tabatabaei Qomsheh (spécialiste en ingénierie nucléaire)

→ En 2025/2026, pour la première fois depuis les années 2010, plusieurs scientifiques sont éliminés en même temps, mais dans un **contexte de frappes militaires ouvertes**. Les cyberattaques et assassinats ont surtout été des outils de guerre clandestine avant 2025. Depuis 2025, ils s'intègrent plutôt dans un conflit militaire direct contre l'Iran.
→ Les frappes aériennes (trois épisodes majeurs en 45 ans) contrastent avec les **opérations clandestines (cyber, sabotage, assassinats), beaucoup plus fréquentes**.