# MoD investigates major security breach after special forces identities leaked online



The Ministry of Defence (MoD) is currently investigating a significant security breach after the identities of members of Britain’s special forces were inadvertently published online. The incident has raised serious concerns over operational security and the safety of elite troops.

Documents containing the names, ranks, and affiliations of at least 20 special forces soldiers were made publicly available on the internet by two publications associated with the British Army. The releasеd information included links revealing some soldiers’ connections to elite units such as the Special Air Service (SAS) and the Special Boat Service (SBS). Notably, these updates to the documents were recent, meaning some of the personnel named might have been actively engaged in live operations at the time the information was disclosed.

The material was originally intended only for members of the armed forces, but it appears the documents were widely disseminated without essential security measures, such as password protection. This oversight has prompted alarm within the defence community. The MoD emphasised that “the safety of our personnel is of paramount importance.” However, the breach has been described as one of the most serious security failures in recent years.

Tom Tugendhat, a former security minister who served in Iraq and Afghanistan, commented on the situation, highlighting the ongoing challenges of safeguarding operational details. Speaking to the Express, he said: “Thirty years ago terrorism coming from Northern Ireland made us all aware of operational security at home. It’s clear that some of those lessons need to be learnt again.”

The SAS and SBS, collectively known by the motto “Who Dares Wins,” are among the world’s most feared and secretive combat units. Their missions often involve covert operations in hostile environments, requiring their actions, identities, and deployment locations to be kept strictly confidential. This secrecy is crucial not only to preserve the effectiveness of missions but also to protect soldiers and their families from becoming potential targets.

Historically, the MoD refrains from commenting on special forces deployments or the identities of personnel involved. Soldiers’ details are carefully guarded to avoid compromising operational security. However, some former special forces members have, at times, voluntarily disclosed their involvement post-service. In this instance, one of the publications went further by revealing a codename linking an individual to the special forces, along with information implying that the individual was overseas on deployment.

This incident follows a previous breach in 2021, when the identities of over 100 special forces personnel were accidentally exposed in a document listing army promotions. Unlike the current event, that earlier disclosure was limited to an email circulated among civil servants and soldiers rather than documents accessible publicly online.

The current breach is being treated with the highest seriousness by the Ministry of Defence, which is conducting a full inquiry into how the documents came to be published without proper safeguards and what steps will be taken to prevent similar incidents in the future. The MoD's response underscores the critical importance of maintaining operational security to protect the nation’s most sensitive military operations and personnel.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.telegraph.co.uk/news/2025/04/27/sas-security-breach-as-serving-soldiers-names-published/> - Confirms the security breach involving the inadvertent online publication of identities of at least 20 British special forces soldiers, including details like ranks and unit affiliations.
2. <https://www.telegraph.co.uk/news/2025/04/27/sas-security-breach-as-serving-soldiers-names-published/> - Details the MoD's response, including taking down the documents and notifying affected personnel, as well as the recent updates to the documents indicating active operational involvement.
3. <https://www.telegraph.co.uk/news/2025/04/27/sas-security-breach-as-serving-soldiers-names-published/> - Explains the absence of explicit unit names but mentions code names for special forces operations, corroborating the article's claim about indirect yet identifiable unit connections.
4. <https://www.kpl-databreach.co.uk/special-forces-data-breach/> - Provides context about the 2021 breach involving over 100 special forces personnel, contrasting it with the current online disclosure of documents.
5. <https://www.kpl-databreach.co.uk/special-forces-data-breach/> - Describes the 2021 incident as an email-based internal mishap, supporting the article's distinction between the current publicly accessible breach and past internal errors.
6. <https://www.telegraph.co.uk/news/2025/04/27/sas-security-breach-as-serving-soldiers-names-published/> - Highlights concerns raised by the breach, including potential targeting by hostile entities, aligning with the article's emphasis on operational security risks.
7. <https://www.express.co.uk/news/uk/2047176/MoD-SAS-SBS-special-forces> - Please view link - unable to able to access data