

# UK Government Probing Cyber-attack over Syria Propaganda Leaks

Ministers alerted after hackers dump details of covert Foreign Office programmes online, with suspicion focusing on Russia

By [Ian Cobain](#)

Global Research, September 30, 2020

[Middle East Eye](#) 28 September 2020

Region: [Europe](#), [Middle East & North Africa](#)

Theme: [Intelligence](#), [US NATO War Agenda](#)

In-depth Report: [SYRIA](#)

*Hackers have penetrated the computer systems of the UK's foreign ministry and taken hundreds of files detailing the country's controversial propaganda programmes in war-torn Syria.*

In a security breach of enormous proportions, the hackers appear to have deliberately targeted files that set out the financial and operational relationships between the Foreign, Commonwealth and Development Office (FCDO) and a network of private-sector contractors that have been covertly running media platforms in Syria throughout the nine-year civil war.

Middle East Eye understands that between 200 and 300 highly sensitive documents are thought to have been acquired by the hackers.

Some of the documents have already been posted on the internet, and foreign office ministers and officials are bracing themselves for the possible appearance of more over the coming weeks.

While the hackers are not thought to have yet been identified, the sophistication of the cyber-attack has raised concerns at the FCDO that a state actor could have been responsible, with suspicion focusing on Russia.

In 2018, [the UK foreign ministry said](#) that Russian intelligence officers had attempted to hack into its computer systems.

The FCDO is refusing to comment on the hacking that led to the exposure of the Syrian propaganda material.

In a statement, the ministry said:

"The UK has been clear in our support for elements of the moderate opposition in Syria to stand up to both the tyranny of the Assad regime and the brutal ideology of Daesh."

The FCDO became aware of the breach last week, after some documents had been posted by the hacking collective known as Anonymous. Foreign Secretary Dominic Raab was briefed at the weekend and other ministers were informed on Monday.

The documents shed further light on propaganda initiatives known in UK government circles as “strategic communications”, whose existence [came to light](#) four years ago, and [which MEE detailed](#) earlier this year.

The programme aimed to promote “attitudinal and behavioural change” among Syrian audiences by fostering secular values, building resilience among the civilian population and by promoting what the UK government described as the Moderate Armed Opposition.

They show that British government contractors established radio stations, published Arabic- and English-language magazines, newspapers, books and children’s comics, designed posters and stickers, and helped to run opposition groups’ media offices.

One contractor is said to have distributed more than 660,000 printed items across Syria in six months.

The hacked documents also show how the “strategic communications” programme has influenced the reporting of many major media organisations, with one contractor claiming to be in contact with 1,600 international journalists and other individuals able to help influence public opinion.

#### Citizen journalists

At the heart of the propaganda initiatives was a large network of Syrian citizen journalists, many of whom began reporting on the uprising against the government in 2011 and were then provided with training, equipment and encouragement by UK contractors – without the role of the British government being made explicit.

A number of citizen journalists were detained and murdered by the Islamic State group after it began capturing territory in the country in 2015.

IS frequently denounced its victims as western “spies”, and some Syrian citizen journalists were pursued across the border to Turkey and murdered.

The documents posted on the internet in recent days identify not only private-sector contractors working for the Foreign Office, but also a number of the individuals who are running those companies.

However, MEE understands that senior FCDO officials are less concerned about the contents of many of the documents – as the existence of the propaganda programme had already been made public – than they are about the apparent ease with which the department’s computer systems were broken into.

Similar programmes have been run in Syria by the UK’s Ministry of Defence, which does not appear to have been hacked.

\*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

The original source of this article is [Middle East Eye](#)

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Ian Cobain](#)

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)

[www.globalresearch.ca](http://www.globalresearch.ca) contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)