GlobalResearch
Center for Research on Globalization

Leaked Files: How Britain Trains Jordan to Spy on Its Citizens

The British government covertly trained Jordanian security services in techniques known as "digital media exploitation" which has been used to monitor, manipulate, and disrupt dissent in the kingdom.

By Kit Klarenberg

Global Research, January 25, 2023
The Cradle 24 January 2023

Region: Europe, Middle East & North Africa
Theme: Intelligence

***

Leaked documents reviewed by The Cradle reveal that Britain secretly trained Jordanian security services in techniques used by the notorious UK security and cyber agency GCHQ, which provides signals intelligence to the British government and its armed forces.

Over three intensive, week-long, Foreign Office-funded training sessions conducted between June 2019 and March 2020, members of the Public Security Directorate's shadowy Special Branch, handpicked by the British Embassy in Amman, were taught the finer points of "digital media exploitation."

In theory, the purpose of the exercise was to assist "evidence gathering agencies in Jordan to effectively extract data from digital devices" to enhance their investigative capabilities, and improve the standard of prosecutions, particularly in the field of terrorism.

This would in turn enable enhanced sharing of evidence between Amman and London, "and lead to increased operational cooperation."

Tried and tested tactics

As readers of *The Cradle* will well-know by this point, the officially stated noble objectives of Whitehall's assorted security support and reform programs in West Asia may not align with the underlying reality of these efforts.

For example, this outlet has previously revealed how British operatives and technology are placed in Lebanon's intelligence services under the guise of teaching them how to use digital forensic tools. This allows London to closely monitor their activities – and Lebanese citizens.

Those programs are delivered by British government contractor Torchlight, a company staffed by UK military and intelligence veterans with high-level security clearances. The same company was also behind the training provided to Jordan's Special Branch.

According to its submissions to the Foreign Office, based on a "comprehensive on-site visit" in 2018, the Directorate's operatives were already "satisfactorily equipped in terms of hardware and software" to conduct "digital media exploitation."

Spying on citizens

However, Torchlight felt that they were not "adequately trained to fully exploit the potential of the equipment they possess." Given the resources available to the Directorate, this "potential" could be highly concerning.

For example, Torchlight has noted that Special Branch uses Cellebrite's suite of digital intelligence products. Cellebrite, an Israeli company with clients including multiple repressive governments, produces technology capable of breaking into encrypted devices and extracting and analyzing all data within it.

While the firm has helped solve murky murder cases, overwhelmingly it is deployed to monitor the activities of human rights activists, journalists and dissidents.

The professional backgrounds of Torchlight staffers involved in the Jordanian training project raise additional concerns. It was led by the company's Head of Digital Intelligence, Andy Tremlett, a cyber and electronic warfare specialist who spent over a decade in senior positions at GCHQ.

Along the way, he was "charged with the provision of support to the most specialized and discreet areas" of British Special Forces operations, and responsible for expanding the agency's "overseas footprint" and "potential delivery platform." These positions granted him "vast experience in how to use and exploit digital material," and integrating different forms of intelligence in broader espionage operations.

'Destroy, deny, degrade and disrupt'

Further details of Tremlett's ability to "exploit" the private data of targets aren't offered, although he is said to have "spent a significant portion of his career within the Joint Threat Research Intelligence Group (JTRIG)." The existence of this unit was exposed by US National Security Agency whistleblower Edward Snowden in 2014, and the details of its operations are truly shocking.

JTRIG's explicit mission is to employ a variety of dirty tricks to "destroy, deny, degrade and disrupt" enemies and "discrediting" them, by planting "negative information" about them online, and manipulating discussions on internet forums and social networks.

A leaked presentation on JTRIG's covert activities shows this harassment extends to changing an individual's social media profile pictures to take their paranoia "to a whole new level" or simply deleting their online presence, writing anonymous blog posts "purporting to be [by] one of their victims" to damage their reputations, emailing and texting their work colleagues, neighbors and friends, and arranging "honey trap" stings.

"A great option. Very successful when it works," the presentation states in regard to the latter strategy. "Get someone to go somewhere on the internet, or a physical location to be met by a 'friendly face.' JTRIG has the ability to 'shape' the environment on occasions."

Writing incriminating blog posts was said to have "worked on a number of different ops," with "Iran work" cited as a particularly effective example, although this is not expanded upon. Elsewhere, it is disclosed that JTRIG "significantly" disrupted the Taliban's communications network by bombarding them with phone calls, texts and faxes "every 10 seconds or so."

Evidently, it was not digital forensics with which Torchlight's training modules were primarily concerned. In fact, JTRIG operations related to "digital media exploitation" were, per the leaked presentation, primarily concerned with placing information on "compromised" electronic devices, including "damning information, where appropriate."

Protecting the British-installed monarchy

In Jordan, criticism of King Abdullah II – a member of the Hashemite dynasty installed on thrones across West Asia by the British following World War I, and himself a British Army veteran – and government officials and institutions is a very serious crime.

Journalists are routinely subject to harassment, arrest and prosecution by authorities for even mildly critical reporting or social media posts. And protests over rising hardship among the general population are becoming more frequent.

The prospect of Amman's secret police being proficient in JTRIG's malicious methods is therefore disturbing by definition. The ease with which they could be abused to ruin the lives of objectors, and/or jail them on bogus charges, is clear.

Britain's willingness to export these techniques to Jordan is not surprising. The strict and widely criticized Cybercrime Law, which restricts freedom of expression online and citizens' right to privacy, makes the country a perfect staging ground for London's nefarious activities elsewhere in West Asia, and helps keep their presence and intentions secret.

For example, from the early days of the Syrian crisis, Britain operated a site located 45 minutes from Amman where fighters in the proxy war were trained. Leaked files related to the project predicted that some of these individuals would go on to join Al-Nusra and ISIS and that equipment would be stolen and used by them.

Despite this, the Foreign Office was unconcerned about these prospects, likely because there was little risk that they, or the training program more generally, would ever be publicly exposed.

*

Note to readers: Please click the share buttons above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image is from The Cradle

The original source of this article is The Cradle

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Kit Klarenberg

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

For media inquiries: publications@globalresearch.ca