GlobalResearch
Center for Research on Globalization

Leaked Catalogue: Vast Array of British Military Spy Gear Offered to U.S. Police

By Sam Biddle
Global Research, September 04, 2016
The Intercept 1 September 2016

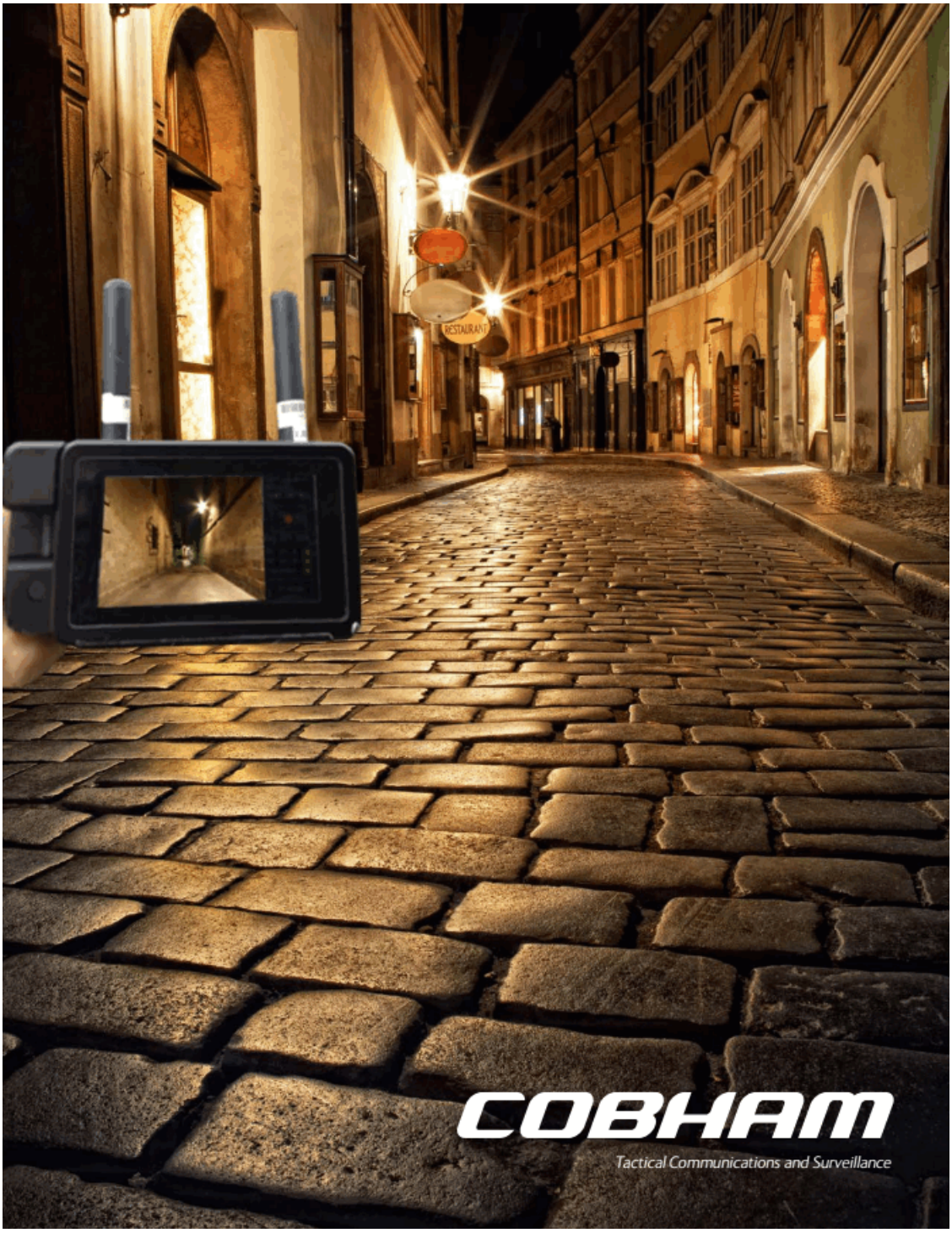
Region: Europe, USA
Theme: Intelligence, Militarization and WMD

A confidential, 120-page catalogue of spy equipment, originating from British defense firm Cobham and circulated to U.S. law enforcement, touts gear that can intercept wireless calls and text messages, locate people via their mobile phones, and jam cellular communications in a particular area.

The catalogue was obtained by *The Intercept* as part of a large trove of documents originating within the Florida Department of Law Enforcement, where spokesperson Molly Best confirmed Cobham wares have been purchased but did not provide further information. The document provides a rare look at the wide range of electronic surveillance tactics used by police and militaries in the U.S. and abroad, offering equipment ranging from black boxes that can monitor an entire town's cellular signals to microphones hidden in lighters and cameras hidden in trashcans. Markings date it to 2014.

Cobham, recently cited among several major British firms exporting surveillance technology to oppressive regimes, has counted police in the United States among its clients, Cobham spokesperson Greg Caires confirmed. The company spun off its "Tactical Communications and Surveillance" business into "Domo Tactical Communications" earlier this year, selling the entity to another company and presumably shifting many of those clients into it. Caires declined to comment further on the catalogue obtained by *The Intercept* or confirm its authenticity, but said it "looked authentic" to him.

"By design, these devices are indiscriminate and operate across a wide area where many people may be present," said Richard Tynan, a technologist at Privacy International, of the gear in the Cobham catalogue. Such "indiscriminate surveillance systems that are not targeted in any way based on prior suspicion" are "the essence of mass surveillance," he added.



2014-Cobham-TCS-Catalog120 pages

The national controversy over military-grade spy gear trickling down to local police has largely focused on the "Stingray," a single type of cellular spy box manufactured by a single company, Harris Corp. But the menu of options available to domestic law enforcement is enormous and poorly understood, mostly because of efforts by both manufacturers and their police clientele to suppress information about their functionality and use. What little we know about Stingrays has often been the result of hard-fought FOIA lawsuits or courtroom disclosures by the government. Whenthe *Wall Street Journal* began reporting on the use of the Stingray in 2011, the FBI declined to comment on the grounds that even discussing the device's existence could jeopardize its usefulness. The effort to pry out details about the tool is ongoing; just this past April, the American Civil Liberties Union and Electronic Frontier Foundation prevailed in a federal court case, getting the government to admit it used a

Stingray in Wisconsin.

Unsurprisingly, the Cobham catalogue describes itself as “proprietary and confidential” and demands that it “must be returned upon request.” Information about Cobham’s own suite of Stingray-style boxes is almost nonexistent on the web. But starting far down on Page 105 of the catalogue is a section titled “Cellular Surveillance,” wherein the U.K.-based manufacturer of defense and intelligence-oriented hardware lays out all the small wonders it sells for spying on people’s private conversations, whether they’re in Baghdad or Baltimore:

The above page immediately stood out to ACLU attorney Nathan Wessler, who has made Stingray-like devices a major focus of his work for the civil liberties group. Wessler said “the note at the top of the page about the ability to intercept calls and text messages (in addition to the ability to geo-locate phones)” is of particular interest, because “domestic law enforcement agencies generally say they don’t use that capability.” Also remarkable to Wessler is the claim that cellphone users can be “tracked to less than 1 [meter] of accuracy.”Tynan said Cobham’s cellular surveillance devices are, like the Stingray, standard “IMSI catchers,” deeply controversial equipment that can be used to create fake cellular networks and swallow up International Mobile Subscriber Identity fingerprints, calls, and texts. But he noted that such devices can operate on a vast scale:

> The Cobham devices in this catalogue are standard interception devices with the ability to masquerade as 1-4 base stations simultaneously. This would allow it to pretend to be 4 different operators or 4 base stations from the same operator or any combination. These specifications allow for the interception of up to 4 calls at a time. The operational distance of these devices would be around 1-2 KM for 3G and significantly greater for 2G devices. Devices of this type can typically acquire the unique identifiers of handsets at a rate of 200 per minute.

Cobham also offers equipment capable of causing immense cellular blackouts and bulk data collection, including the “3G-N” — operated via laptop:

The mammoth “GSM-XPZ PV,” meanwhile, has a maximum output power of 50W, which would make it comparable to cellular antennae constructed by the likes of AT&T or Verizon. Anyone inside its radius (potentially miles from the box itself) could be subject to invisible surveillance.

The slimmer “GSM-XPZ HP Plus,” which appears to be operated via a handheld device, can “take control of target phones” and “create [an] exclusion zone to deny GSM network coverage,” the catalogue states.

Also noteworthy are two “direction finding units” — trackers used for following the location of someone’s smartphone (and presumably its user). One, named the “Evolve4-Hand Held Direction Finder,” actually allows a soldier or neighborhood police officer to carry a hidden antenna inside his clothing that he can use to track someone’s whereabouts:

Another, similar device uses a larger antenna that can be mounted onto any car — a design that raises an eyebrow for Wessler: “The low profile means that it is difficult to identify police use of the technology.”

This low-profile technology not only allows agents in a vehicle to track someone’s location via their mobile phone, but it is also “designed to work with any GSM manipulation,” presumably meaning cellular jamming and interception.

Tools for covert spying make up a large part of the catalogue, particularly in the audio and video surveillance sections, where sensors are hidden in everything from pocket knives and birdhouses to suspenders:

Elsewhere in the catalogue, Cobham boasts of a corporate history going back more than 70 years, brags about tripling in size since 1997, and talks about “clients and partners in over 100 countries.” Among the company’s stated goals are “to keep people safe and to improve communications.”

But the proliferation of spy tools like those sold by Cobham is actually eroding safety, according to Tynan. “As we move to a more connected world where cars, toys, fridges, and even implantable devices contain miniature cellphone technology, the capability to cause harm using one of these devices becomes ever greater,” he said. “It is unacceptable for our modern critical infrastructure to be so vulnerable to such interception,” and therefore “it is vital that the international standards that underpin our communications are built to the highest security standard possible.”

Correction, Sept. 2: The original version of this story misstated the relationship between Cobham and Domo Tactical Communications.

Articles by: Sam Biddle