GlobalResearch
Center for Research on Globalization

Documents Show Private Intelligence Web Behind Global Surveillance Program

By Max Blumenthal
Global Research, June 14, 2018
Truthdig 5 June 2018

Region: Middle East & North Africa
Theme: Intelligence, Media Disinformation, US NATO War Agenda

Internal documents exclusively obtained by the Grayzone Project (and embedded after this article) show how Cambridge Analytica's UK-based parent company, SCL group, conducted a surveillance operation in Yemen called Project Titania. The initiative relied on psychological profiling, "strategic communications campaigns," and infiltration of foreign operatives into indigenous communities through unwitting local partners whom they were instructed to deceive.

According to the materials detailed here, Project Titania was to be implemented by SCL "on behalf of Archimedes." Archimedes is a US-based private contractor that advertises its ability to provide "Systems Integration, Engineering, and Mission Support solutions to government and businesses worldwide."

The partnership between SCL and Archimedes highlights the seamless web of relationships between private intelligence firms and Western governments engaged in counter-intelligence activities in the Middle East. These large scale surveillance operations have been conducted without the knowledge of the Western public or input from elected officials, and would have remained mostly unknown had a series of leaks and hacking operations not placed them in the public domain.

Communications obtained legally by the Grayzone Project indicated that a former Archimedes staffer named Tim Riesen was a key contact for the Yemen operation. Little information is publicly available about Riesen; he is currently the the CEO of an international corporate consultancy firm called Madison Springfield, Inc.

While he is also listed as an adjunct political science professor at the school of graduate studies at Norwich University, a private military academy in Vermont, published material by Riesen is difficult to find online. Riesen did not respond to an interview request delivered by the Grayzone Project to his email at Madison Springfield.

One of Riesen's few public appearances consists of a brief cameo in a 2011 video by AFRICOM, the US military command center that operates in 53 African countries. In the video below, an AFRICOM staffer describes a briefing Riesen delivered on the demographics and political tendencies of South Sudan ahead of its independence referendum that year.

Despite his negligible online footprint, or perhaps because of it, Riesen has made himself a considerable player in the world of private intelligence. That is clear from the tranche of emails that surfaced when the private intel firm HBGary was hacked in 2010 by the

Anonymous collective.

The HBGary hacks were first reported by journalist Barrett Brown, who was prosecuted by Obama's Department of Justice and sentenced to five years in prison for publicizing the emails. When their contents were published in full at Wikileaks, HBGary and consortium of intelligence firms were exposed for planning to carry out a full-scale attack on American social justice activists and journalists.

The firms homed in on journalist Glenn Greenwald and Wikileaks, plotting to undermine both through a campaign of "disinformation," spawning internal rifts and "creating messages around actions to sabotage or discredit the opposing organization." HBGary was also considered by the US Chamber of Commerce to launch a smear campaign against its critics.

In a separate initiative, HBGary aimed to develop a "persona management" system for the US Air Force that enabled users to spam social media with replies from users with false but detailed personas that gave the impression of organic consensus. The project outlined in the emails closely resembles the kind of troll and bot farms that have gained infamy amid America's furor over Russian meddling, however, this one was made in the USA.

According to Barrett Brown, the contract for the system was ultimately won by a subsidiary of Cubic, a major multi-national arms, combat training company, and infrastructure company.

Archimedes and the ROMAS/COIN mass surveillance plan

Though the HBGary emails generated a brief flurry of media interest, little attention was devoted to one of the most disturbing programs they exposed. In a series of communications between intelligence firm directors, an operation came to light that Brown described as "a secretive and immensely sophisticated campaign of mass surveillance and data mining against the Arab world, allowing the intelligence community to monitor the habits, conversations, and activity of millions of individuals at once."

That plan was Romas/COIN, with "COIN" referring to counter-intelligence — the same acronym used in the FBI's notorious COINTELPRO program. Riesen's Archimedes was a key player in the development of the initiative.

According to details of the program gathered by Brown and a collection of online researchers, Apple was also an active team partner, communicating regularly with HBGary CEO Aaron Barr and his peers. In one email, Apple's "Homeland Defense Manager" Andy Kemp rescheduled a meeting with Barr by explaining,

> "I've been requested to be [in] phoenix by a senior member at ODNI [the Office of the Director of National Intelligence] – someone That I don't say no to."

Romas/COIN focused heavily on mobile phone software and applications. Its designers aimed to develop specialized "social media monitoring tools" and linguistic analysis systems, presumably to surveil the communications of younger, activist-minded Arabs on platforms like Facebook.

To emphasize the Arab-centric nature of Romas/COIN, Chris Clair of the intelligence firm

TASC proposed a bold name to his colleagues:

> "Can we name COIN Saif? Saif is the sword an Arab executioner uses when they decapitate criminals. I can think of a few cool brands for this."

In the end, the private spies agreed to call their program "ROMAS."

> "ROMAS is the name of a middle eastern spider. ? I thought I was pretty clever," HBGary's Barr wrote. "I am glad they are going to continue to use the name."

Riesen appears in several emails with Clair, Barr, and a handful of partners pursuing what he called a "potential collaboration opportunity." He described his company, Archimedes, and Barr's HBGary, as subcontractors to Clair's TASC on the project.

Together, they brainstormed a plan to compete with the contractor Northrup Grumman for a lucrative contract from an unnamed US government client seeking advanced capabilities in surveillance and "IO" — the acronym for influence operations.

On July 23, 2010, the ROMAS/COIN team decided on an informal setting to brainstorm their proposal.

> "And we are on Thursday," Clair informed Riesen. I'll have the steaks ready to grill and the beer will be chilled. I am sure it will be loads of fun."

Massive State Department contracts to SCL for covert propaganda

In a recent exchange at the US State Department, spokesperson Heather Nauert confirmed that the US government had provided SCL with lucrative contracts to advance its propaganda goals on the international stage. Nauert acknowledged that in late 2016, the US State Department's Global Engagement Center was granted a $120 million budget to wage war on online ISIS recruitment and Russian "disinformation."

The counter-propaganda initiative promptly doled out two contracts, totaling $496,232, to SCL in February and March of 2017 to carry out "target audience research." According to Nauert, the contracts to SCL were aimed at supplementing US anti-ISIS operations in the Middle East.

Before folding into Emerdata, SCL removed endorsements from NATO and the State Department from its website (image from NBC News)

The Global Engagement Center is an international influence operation run out of heart of the State Department. Originally formed as the Center for Strategic Counterterrorism Communications, and with a mission initially focused on fighting ISIS-oriented propaganda, the operation shifted its focus — and massively expanded its budget — as soon as the national panic over Russian meddling erupted during the 2016 election.

According to Richard Stengel, the center's former director,

> "we supported credible counter-Russian voices in the region. We pretty much stopped creating content ourselves."

Which voices Stengel was referring to remains unclear, but as the former managing editor of Time Magazine, his remarks raised questions about whether the US government was covertly paying or promoting journalists to advance its agenda in Eastern Europe.

At a Council on Foreign Relations forum on "fake news" this May, Stengel made an unusually candid disclosure.

> "My old job at the State Department was what people used to jokingly [call] the chief propagandist job," he declared. "I'm not against propaganda, every country does it and they have to do it to their own population and I don't necessarily think it's that awful."

> At a Council on Foreign Relations forum about "fake news," former Editor at Time Magazine Richard Stengel directly states that he supports the use of propaganda on American citizens – then shuts the session down when challenged about how propaganda is used against the third world pic.twitter.com/ClAT5POv7G
>
> — William Craddick (@williamcraddick) May 11, 2018

Rebranding a toxic name

Just weeks after the collapse of Cambridge Analytica and SCL, the firm's principals, including Rebekah Mercer, magically resurfaced as directors of a newly minted, London-based company called Emerdata that appears to differ from SCL in name only. In fact, the firm is even headquartered at the same office formerly occupied by SCL Elections.

The brazen rebranding of SCL/Cambridge Analytica might be disturbing, but these firms are only part of a much wider web of private intelligence firms determined to manipulate the behavior of the public for the benefit of powerful clients. And before these cynical operators applied their methods in Western elections, they tested them on populations in conflict zones like Yemen.

Back in 2011, when he exposed the Romas/COIN mass surveillance program, Barrett Brown warned of the coming blowback for the West.

> "It is inevitable, then, that such capabilities as form the backbone of Romas/COIN…will be deployed against a growing segment of the world's population," Brown wrote. "The powerful institutions that wield them will grow all the more powerful as they are provided better and better methods by which to monitor, deceive, and manipulate. The informed electorate upon which liberty depends will be increasingly misinformed. No tactical advantage conferred by the use of these programs can outweigh the damage that will be done to mankind in the process of creating them."

*

Max Blumenthal is the editor of the GrayzoneProject.com and the co-host of the podcast Moderate Rebels. He is an award-winning journalist and the author of books, including the best-selling "Republican Gomorrah: Inside the Movement That Shattered the Party," "Goliath: Life and Loathing in Greater Israel" and "The Fifty One Day War: Ruin and Resistance in Gaza."
