THE GEOSTRATEGIC AND HISTORIC IMPLICATIONS OF CRYPTO

If you haven't already, you should read the superb WaPo story on Crypto, the Swiss encryption company that German and US intelligence agencies secretly owned, allowing them to degrade the encryption used by governments all over the world. The story relies on classified CIA and BND histories obtained by the paper and a German partner.

> The decades-long arrangement, among the most closely guarded secrets of the Cold War, is laid bare in a classified, comprehensive CIA history of the operation obtained by The Washington Post and ZDF, a German public broadcaster, in a joint reporting project.
>
> [snip]
>
> The Post was able to read all of the documents, but the source of the material insisted that only excerpts be published.
>
> The CIA and the BND declined to comment, though U.S. and German officials did not dispute the authenticity of the documents. The first is a 96-page account of the operation completed in 2004 by the CIA's Center for the Study of Intelligence, an internal historical branch. The second is an oral history compiled by German intelligence officials in 2008.

From the 1970s until the early 2000s, the company ensured its encryption had weaknesses that knowing intelligence partners — largely the NSA — exploited. CIA retained control of the company until 2018.

The WaPo correctly puts Crypto in a lineage that includes later spying and politicized fights over which corporations run the global telecommunications system. But it curiously suggests that the US "developed an insatiable appetite for global surveillance" from the project, as if that's a uniquely American hunger.

> Even so, the Crypto operation is relevant to modern espionage. Its reach and duration helps to explain how the United States developed an insatiable appetite for global surveillance that was exposed in 2013 by Edward Snowden. There are also echoes of Crypto in the suspicions swirling around modern companies with alleged links to foreign governments, including the Russian anti-virus firm Kaspersky, a texting app tied to the United Arab Emirates and the Chinese telecommunications giant Huawei.

Any nation-state or powerful non-state actor is going to want access to as much information as it can obtain. Russia, the Gulf states, and China, as well as the unmentioned Israel, are no different.

The story is better understood, in my opinion, as a lesson in how the US, Cold War partner Germany, and several key individuals and companies who could be motivated by Cold War ideology accomplished its spying. It absolutely provides important background to current US efforts to prevent rivals from achieving hegemony over communication structures. But if you didn't know the US is so worried about Huawei's dominance because it gives China a way to supplant the US spying footprint, you're not paying attention.

Some particular features:

- Crytpo was a Swiss company. That gave it some plausible

deniability.

- The operation struggled to find cryptologists who were good, but not too good. People who could identify weaknesses in the algorithms Crypto used either had to be fired or bought off.
- The entire scheme worked off a corruption of market forces. The predecessor to Crypto sold shitty encryption to disfavored countries, but the US made up for the lost profits. Then, as integrated circuits presented a challenge for the business, the US leveraged that to get ongoing cooperation. Then CIA and BND bought out the company via a shell company set up in Lichtenstein. To sustain its customer base, Crypto would smear competitors and bribe customers with gifts and prostitutes.
- The US leveraged its power in the US-German partnership at the core of the operation, forcing the Germans to sell degraded products to allied governments.
- The ideology of the Cold War proved a powerful motive for

> some of the key participants, leading them to work for what ultimately was the CIA for no additional funds.

Those features are worth noting as you consider where this capability moved to as Crypto became less valuable:

- AT&T and other US backbone providers
- Silicon Valley companies compelled under Section 702 of FISA
- Various products supported by CIA's investment arm, In-Q-Tel
- SWIFT

702 is the big outlier — in that the US government leveraged existing market dominance and actually didn't hide what was going on to those who paid attention. But that's changing. The US government is increasingly demanding that its 702 partners — notably both Apple and Facebook — make choices dictated not by a market interest in security but by their demands.

The WaPo story cites some "successes:" nearly complete visibility on Iran, a critical advantage for the UK in the Falklands war, and visibility on Manuel Noriega as he started to outgrow his client role. One wonders what would have happened if the US or its allies had lost visibility on all those key strategic points.

WaPo focuses its challenge to this spying, however, on what the US had to have known about but overlooked: assassination, ethnic cleansing, and atrocities.

> The papers largely avoid more unsettling questions, including what the United States knew — and what it did or didn't

> do — about countries that used Crypto machines while engaged in assassination plots, ethnic cleansing campaigns and human rights abuses.
>
> The revelations in the documents may provide reason to revisit whether the United States was in position to intervene in, or at least expose, international atrocities, and whether it opted against doing so at times to preserve its access to valuable streams of intelligence.
>
> Nor do the files deal with obvious ethical dilemmas at the core of the operation: the deception and exploitation of adversaries, allies and hundreds of unwitting Crypto employees. Many traveled the world selling or servicing rigged systems with no clue that they were doing so at risk to their own safety.

I'm actually more interested in the latter case, though (though after all, the US was overlooking atrocities in Iran, Panama, and Argentina, in any case).

These atrocities were known in real time, but ideology — largely, the same Cold War ideology that convinced some of the engineers to play along quietly — served to downplay them. The ideology that excuses much of our current spying, terrorism, likewise leads many to excuse Americans and allies overlooking atrocities by our allies (but that, too, is evident without proving they're reading the SIGINT proving it).

But the solutions to this problem have as much to do with fixing ideology and market forces behind the power structures of the world as it does with protecting the encryption that people around the world can access.