CIA vs. Wikileaks

Intimiditation surveillance and other tactics observed and experienced

Remote Chaos Experience, 2020-12-28

Andy Müller-Maguhn, amm@wauland.de

Disclaimer 1

- Working as a journalist around the topic of surveillance, signal intelligence, data security etc for > 20 years, this talk goes a bit beyond things *“observed”* and *“analyzed”* as I’m describing events where i have been targeted. While I might not be the most neutral person in this situation, I’m trying to be technically as accurate as possible.
- I have been addressing human rights issues in the digital age for a long time and co-founded EDRI exactly to ensure the enforcement of human rights also in the digital environment. What happened here however is a dimension beyond digital rights; it goes into real life. While I’m a german citizen, I welcome any support to analyse it from the perspective of the universal human rights perspective to address the issues also for other victims.

Disclaimer 2

- This talk addresses activities of CIA and most propably other intelligence activities against persons who have been surrounding and/or in contact with Julian Assange and/or other members of Wikileaks
- The concrete events described **are personally observed / experienced** and therefore at best a small fragment of the complete picture.
- Other persons – with similar or even more crass experience – exists but circumstances do not suggest to disclose at the moment.

Talking Points Overview

- How to get into such a mess
- Context and Timeline
- Psychology; Paranoia vs. Cognitive Dissonance
- The new normal of “IT-Incidents”
- Covert vs. Overt; intimidation surveillance
- Physical Events and their impact
- The elephant in the room and the problem of the missing socks
- Am I infectious? Implications
- How to get out of this mess?

How to get into such a mess

- All Information should be free.
- Free flow of information as a requirement for world peace.
- Self-Conception of 20 years CCC already (when Wikileaks started)
- **The concept of Wikileaks as a democracy test for governments**
- Cultural Missunderstandings of the word “Conspiracy”
- Supporting Media with processing Data and Information
- Working in Journalism is also not always about making friends

Context and Timeline

- Wau Holland Foundation collects donations for WL since 2010
- The publication of AF / IQ Warlogs, the diplomatic cables, the collateral murder video etc. has already triggered legal investigations in the US since 2010 (and ofc arrest of Manning :/)
- Human mistakes have been exploited ever since
- WL published CIA documents in 2017 and the “Vault 7” series
- Pompeo – then still director of the CIA - got very upset; there is 2 references to this – one from 2017-04, another from 2018-02

2017-04-13 Mike Pompeo speech at CSIS (Washington)

(https://www.csis.org/events/discussion-national-security-cia-director-mike-pompeo-0)

"[…] And that is one of the many reasons why we at CIA find the celebration of entities like WikiLeaks to be both perplexing and deeply troubling. Because while we do our best to quietly collect information on those who pose very real threats to our country, individuals such as Julian Assange and Edward Snowden seek to use that information to make a name for themselves. As long as they make a splash, they care nothing about the lives they put at risk or the damage they cause to national security.

WikiLeaks walks like a hostile intelligence service and talks like a hostile intelligence service. It has encouraged its followers to find jobs at CIA in order to obtain intelligence. It directed Chelsea Manning in her theft of specific secret information. And it overwhelmingly focuses on the United States, while seeking support from anti-democratic countries and organizations.

It is time to call out WikiLeaks for what it really is – a non-state hostile intelligence service often abetted by state actors like Russia. In January of this year, our Intelligence Community determined that Russian military intelligence—the GRU—had used WikiLeaks to release data of US victims that the GRU had obtained through cyber operations against the Democratic National Committee. And the report also found that Russia's primary propaganda outlet, RT, has actively collaborated with WikiLeaks. [...]"

2018-02-16 Pompeo speech at the MSC (Munich)

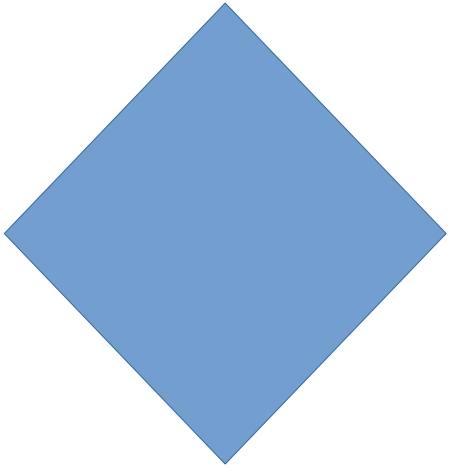
“Intelligence Roundtable”

“[…] Wie in Trumps Regierung allerdings über WikiLeaks gedacht wird, zeigt ein vertraulicher Vortrag des damaligen CIA-Chefs Mike Pompeo im Frühjahr 2018 vor Geheimdienstkollegen. Er verbringe “einen Großteil meiner Zeit damit”, sich nicht-staatlichen Gegnern zu widmen, “sei es Al-Kaida oder Isis, sei es Wikileaks oder Hisbollah” sagte Pompeo. Die genannten Gruppen arbeiteten allesamt daran, “unsere Organisationen zu zerstören. [...]”

(Quelle: Die Zeit vom 17.04.2019)

Psychology; Paranoia vs. Cognitive Dissonance

Real Cause



Cognitive Dissonance
(all-is-fine simulation)

Paranoia
(seeing patterns)

Cover Story based on
plausible deniability

The new normal of “IT-Incidents”

- The quality and amount of IT-Incidents are better to be put into a separate report
- Basic Patterns observed:
  - Attack on encrypted connection in correlation with events
  - Mobile Phones with Data Service (IP) an issue
  - LTE downgrade attacks to 3G, followed by attacks there on IP level
  - Fixed Line issues with TLS-Certificates when using VPN
  - Attack on GPG-/PGP-Keys of communication partners

Covert vs. Overt; intimidation surveillance

- From at least 2017-06 on, questions and treatment at the UK border changed:
  - (1) “Do you live in the UK?” / Alternative: “What is your occupation?”
  - (2) “How long do you stay?”
  - (3) “What do you do in the UK?”
- Later I realized that the border police uncle did not even listen to my answers, sometimes repeated question1 after answering question3. Turned out to be a delay tactic until green light on the screen; propably “team to follow me through my stay” was ready :/
- British surveillance much more offensive when counter-observed (not backing off to not risk beeing outed)
- Cars following at 3 o’clock in the night in one-way streets ..
- New favourites: homeless looking people on the street with cheap plastic bags hiding digital cameras with zoom :/
- At some point it is no more covert at all, pure overt intimidation; creating “state of distress” [see manual]

Physical Incidents and their impact

- Incidents1: 2018-03-23 (revealed)

  Found physical bug in Cryptophone (modified Snom 870)

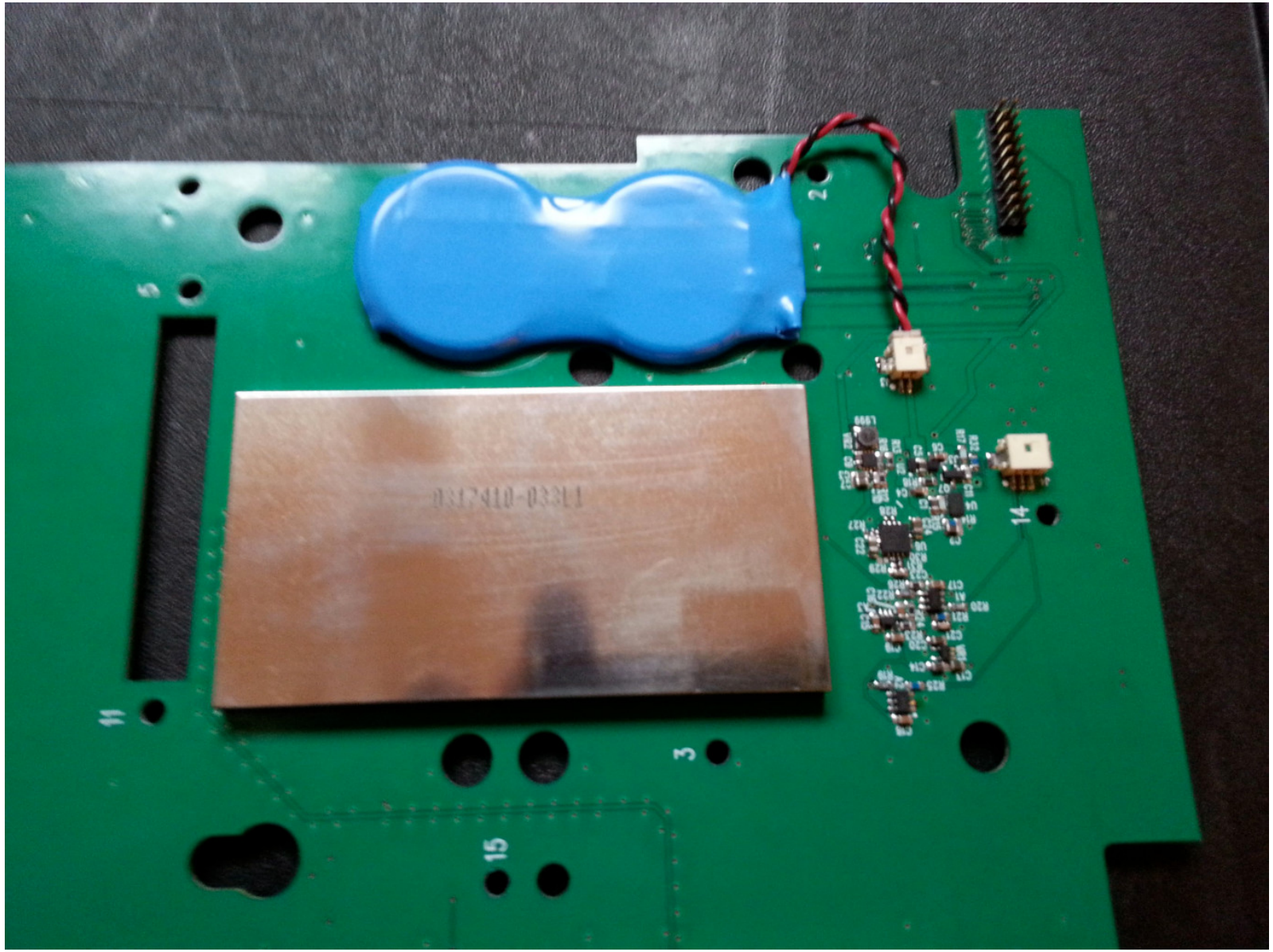
  - opened device to replace faulty display (unrelated cause)

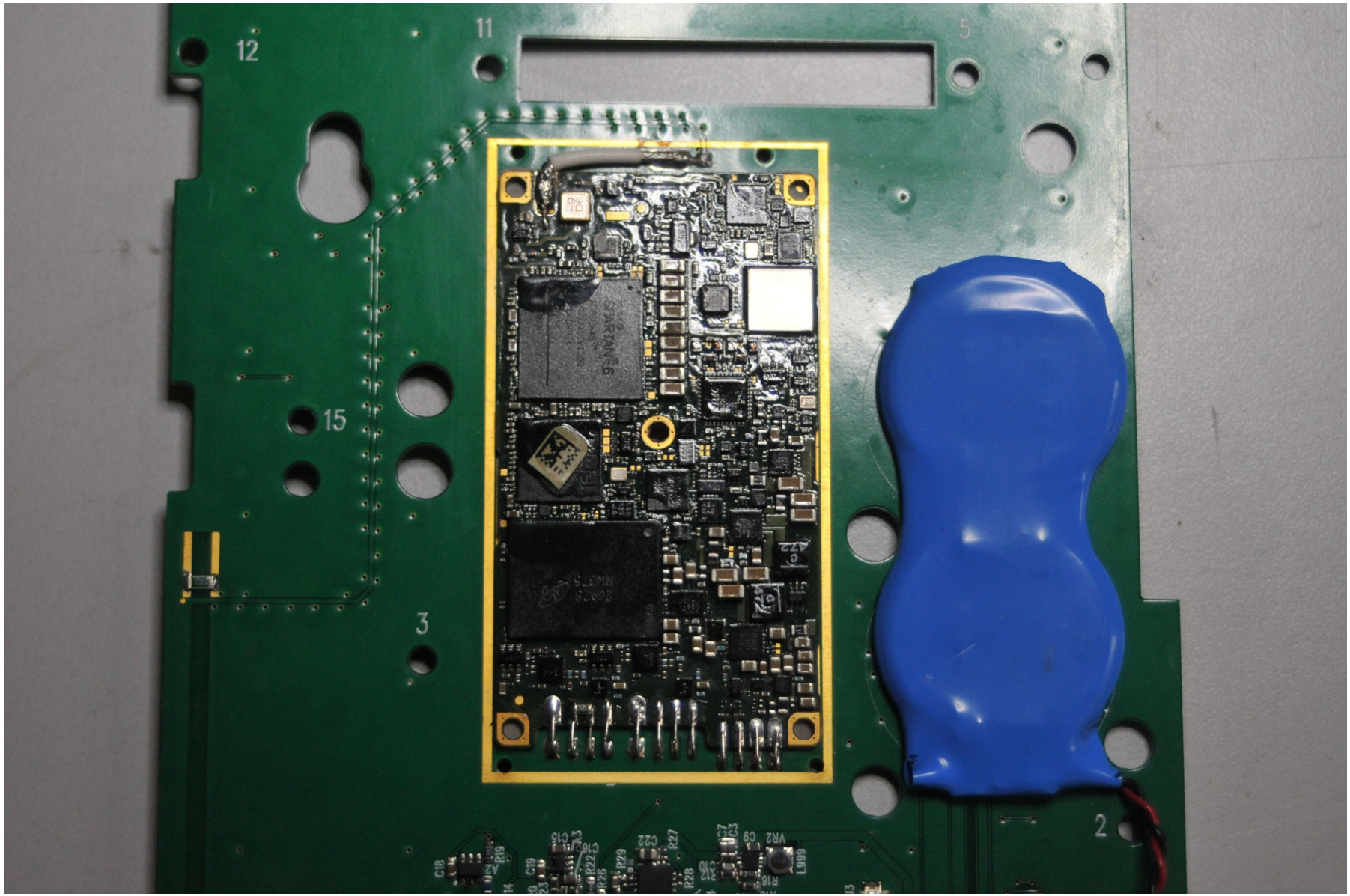
  - found modified keyboard PCB with integrated module

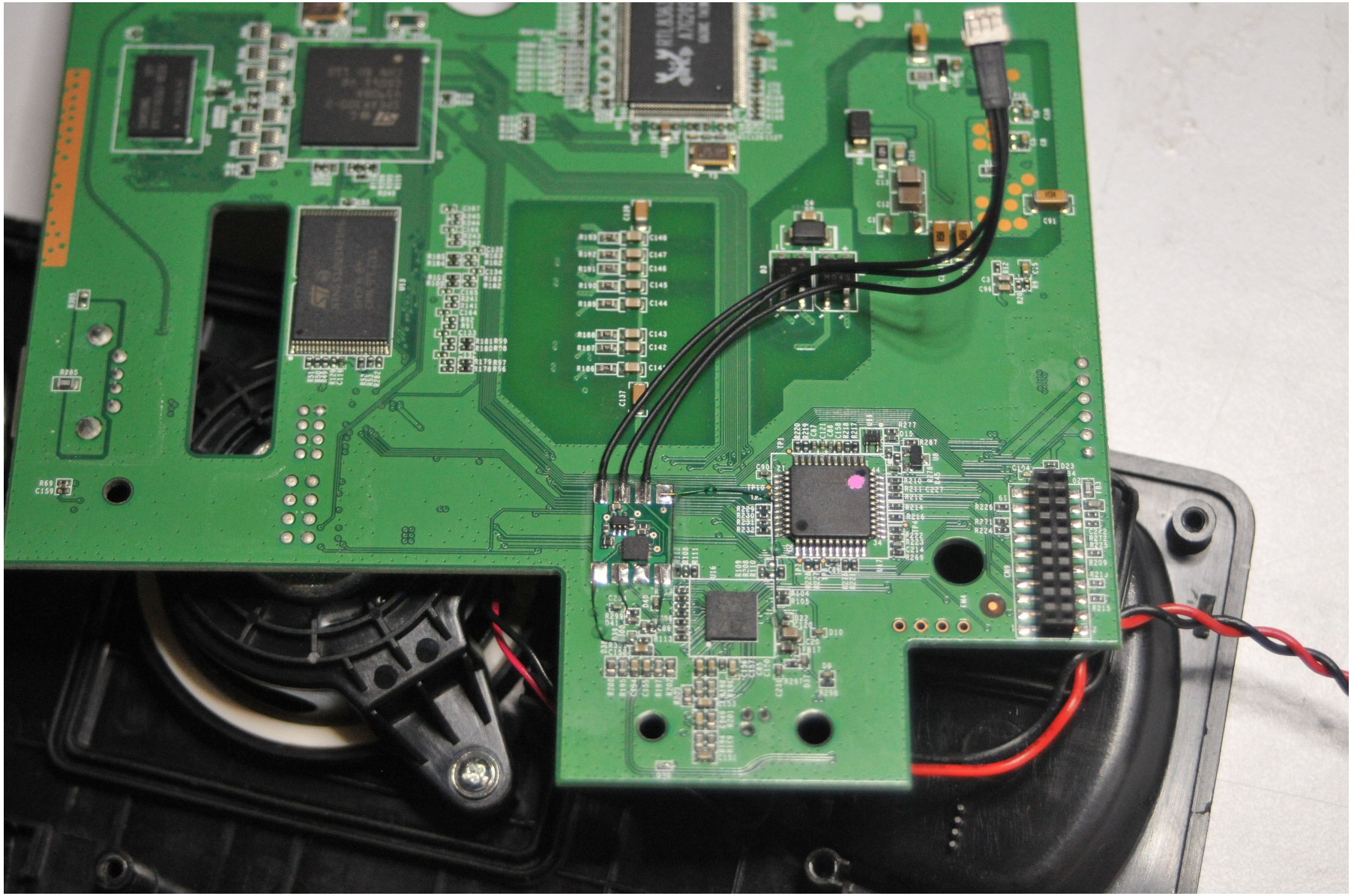
  - FPGA based design + HW crypto, 16 Gb Flash Rom..

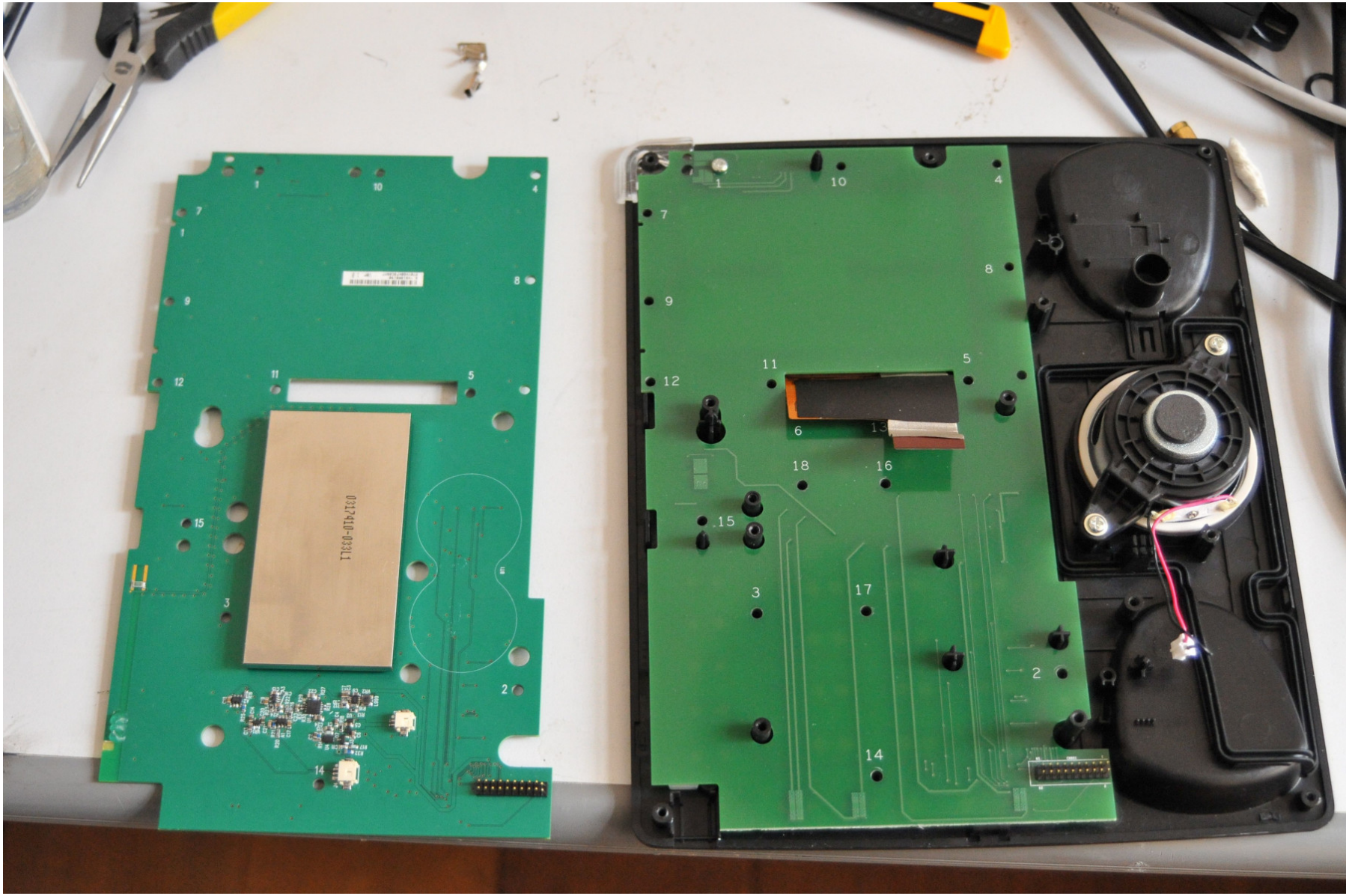
  - hf passive, receiving, triggered activation + transmission

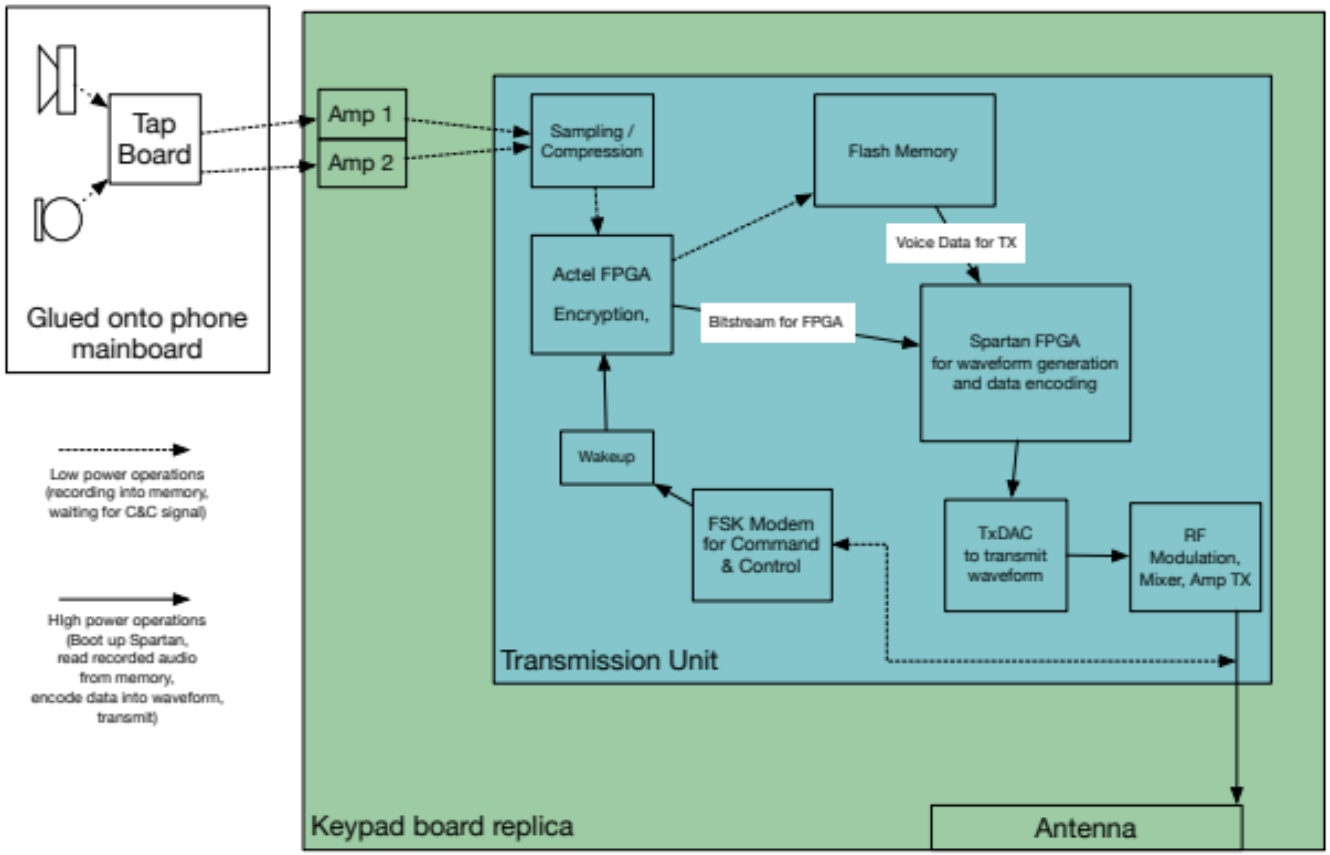
  see http://buggedplanet.info/lost+found/20180323/




12
11
5
15
3
2







Preliminary functional diagram of the major components of the listening devices. Power, lithium battery and charging components omitted.

Aspects of Incident1

- Timeframe of operation: completely unclear, could be years
- (Components produced from ~ 2013-04 on)
- Dimensions suggest non-metric origin
- Antenna around 800 Mhz
- SCS / TAO + physical = CIA PAG (Physical Access Group) [34038.pdf]
- Single Unit deployment unlikely → what else?
- Hard confrontation with Cognitive Dissonance

Physical Events and their impact

- Incident2: 2020-11-03 (happened)

  Tampering with appartment door lock

  Went out in early morning just for about 30 mins (~07:10 - 07:40)

  (Realized closed surveillance team afterwards :/)

  When coming back: Stealth-Key did not fit in Cylinder, Object inserted

  $FriendfromLockIndustryChecked with Police

  → Ongoing investigation

Aspects of Incident2

- Was the Cylinder maybe opened in a destructive way and replaced?
- Was is a trap to make *me* replace the tampered cylinder with one that is less-difficult to open with lockpicking-ways / for intel actors?
- Was the whole incident not about the door, but about to freak me out?
- How much of my **time** did the incident eat that prevented me from realizing potential other events in that timeframe?
- Should I name Pompeo as a suspect? Is it related to the Date?

Physical Events and their impact

- Incident3: 2011-02 (shipped) till 2011-04 (arrived)

  Legal Documents shipped from Berlin (DE) to Madrid (ES) by DHL-Express in the context of the case against UC Global suspect to have been working for the CIA (see my last years talk about the surveillance in the embassy).
- Documents in a sealed bag, with a list of contents outside in a white envelope, that envelope also sealed and put in a DHL-Express envelope
- See pictures of what arrived: all opened, photographed
- Spanish lawyers had also a collection of incidents, some more serious (break-in into their office, intruders blacking out CCTV cams as first step)

  → Ongoing investigation


ZOLL
ZOLL
DHL
Shipment Waybill
(Non negotiable)
DHL Servicepoint
866 4168 170
dhl.com


ZOLL
ZOLL

Aspects of Incident3

- Breach of attorney-client privilege (“Anwaltsgeheimniss”)
- Was german customs (“Zoll”) involved or just their duct-tape?
- Why did the email with my report to my lawyer got deleted and ended in the trash of my lawyer (costing few days delay)
- (he realized!) → [...]
- Why does DHL refuse to name entity and legal grounds?
- Is it potentially again just stealing time and attention?

The elephant in the room and the problem of the missing socks

- Pompeo & the CIA seem a bit over-present on my cognitive systems
- How to deal with the real life problems occuring through such a situation?
- (Suspect the bedsheets first!), but default option:
- *The CIA is reponsible for everything including the missing socks*
- While making jokes about this (escapism) might be ridiculous, if staying serious all-the-time about it helps to stay sane is also unclear.
- Maybe I should invite more friends to my ~~office~~ laboratory for surveillance to deal with the elephant in the room(s)? Ideas?
- Important seems however also to not auto-respond to provocations.

Am I infectious?

- Having gone through this experience creates hypersensitivity and ongoing situational awareness. It’s no more “sometimes”.
- The ability to enjoy any “*ignorance is a bless*”-type of cognitive dissonance is limited with the next fnord and by the ongoing state of distress :/
- If that wouldn’t be enough, people I interact, work or share space-time with and/or communicate even harmless things report that their phones crash, secure messenger apps disappear and/or start to observe weird things
- Internalizing stress is one thing to do for yourself, but not always possible for others.

How to get out of this mess?

- Option1:

  I manage to get proper authorities to make the CIA stop acting in illegal ways against me and other persons surrounding.

- Option2:

  Pompeo reads and understands Mark 4:22, realizes the wrongdoing against Julian / WL and all people targeted in that context and stops it.

- Option3:

  Maybe you out there have some ideas?