Published in *Continent.*, 2019, issue 8.1-2, pp. 176-185, which should be cited to refer to this work.



# Remaking an IMSI catcher

Félicien Goguey

In 2014, several articles on the Web described « mysterious » cell towers intercepting phone calls in the United States. Soon after, the public began speculating about the purpose of such interceptions and who was conducting them (Farman, 2016). With the appearance of this technology emerged a multitude of dubious and suspicious imaginaries. Today, those « mysterious » and « dummy » towers are known to be IMSI[1] catchers (also known as Stingray in North America).

These monitoring devices intercept mobile phones IMSI and conversations of their users by mimicking the activity of a cell tower. The way they operate is based on a man-in-the-middle attack: « an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other »[2]. The use of IMSI catchers to intercept cell phones identity and conversations of their users emerged in the mid-nineties (Strobel, 2007). They are known to be used in counter-terrorism and anti-crime operations but also during protests and as industrial spying tools among others. More recently, in post terror attacks contexts, the use of such devices has been legalized in many countries, such as in France (2015) and Switzerland (2016). Nonetheless, public budget documents have revealed that French customs intelligence services bought IMSI catchers as early as 2010 and 2014[3] (when their use was illegal). Yet, little is known about their existence and their own functioning by the public.

For Allen's term "apocryphal technology", we refer to "technological imaginaries that are more explicitly dubious, suspicious, or fraudulent" (Allen, 2018). He assumes that "all technologies contain at least some element of apocrypha, as they always comprise functions or benefits that exceed their limitations in the here and now." In this sense, IMSI catchers can be seen as a kind of an apocryphal technology: with their use and their opaque and hidden nature emerge various incorrect assumptions and misrepresentations about what they can do, or might do.

How can we, as researchers, study such an entity? Jentery Sayers has argued the relevance of remaking old technologies in media studies and digital humanities (Sayers, 2014). More precisely, he developed a typology in which he describes several matters for which the remaking process is relevant: « composition », « assembly », «

interface », « failure », « abstraction », « instrumentalism » and « speculation ». Although the IMSI catcher is a contemporary technology instead of a past one, there is little to be found about the way it operates, and a lot of speculation emerges around what it is capable of. One way to address the apocryphal character of the IMSI catcher is to rebuild it through an iterative design process using multiple pieces of hardware and software. Indeed, the remaking process can help one to better understand how a technology actually works, how it is build or implemented, as well as its limits. Then, this process can be a manner of « exposing the (inadvertent or intentional) misrepresentations and the (naïve or willful) misinterpretations that surround technological developments. » (Allen, 2018).

In light of (1) the lack of sources regarding IMSI catchers and their design, that raises transparency issues and contributes to its apocryphal character; this paper will (2) present the different versions of IMSI catchers that I have remade; and (3) discuss the relevance of such a methodology in regards to Sayers' historical approach for an apocryphal technology[4]. Finally (4), I tackle the pertinence of remaking in regards to a design fiction approach to deal with such myths.

**1. Sources (lack of)**

The IMSI catcher is a relatively new object of surveillance that appeared in the mid-nineties, but its use has been kept secret until recently and is still not known by the public at large (as it is often the case for surveillance apparatus). Multiple reasons make the IMSI catcher an unfamiliar object. First, as media scholar, Jason Farman writes about man-in-the-middle surveillance: « interception troubles the traditional spatial metaphors for surveillance » (Farman, 2016). Thus, it is almost impossible for the people being watched to know if they are observed, or what's going on; with man-in-the-middle attacks, a new regime of confidentiality appears that makes the surveillance even more opaque. Secondly, the cellphone infrastructure plays a big role in the ignorance of the IMSI catcher as it is also opaque itself. As media scholar, Lisa Parks argues, « most people are socialized to know very little about the infrastructures that surround them in everyday life. […] infrastructures are often designed purposefully to be invisible or transparent, integrated with the built environment, whether submerged underground, covered by ceilings and walls, or camouflaged as 'nature'. » (Parks, 2012). IMSI catchers benefit from the same camouflage: they are never seen and hardly detected (Parks, 2016). Another reason is the confidential character of the device. Indeed, it is quite hard for cellphone users to find information or documentation about the actual existence and the use of IMSI catchers, except from leaked catalogues from companies who sell them. Then, it is not surprising to see speculations and misrepresentations emerging around IMSI catchers, and it is not uncommon to read titles like « Mysterious Fake Cellphone Towers Are Intercepting Calls All Over The US »[5] or « Mystery Stingray devices discovered in Washington »[6] in the press.

In Swiss and French law texts, the devices are never designated as IMSI catchers but as « special technical devices for surveillance of telecommunication correspondence »[7], as « technical device allowing the localization in real-time of a person, a vehicle or an object »[8], or as « a technical device to intercept correspondences emitted or received by a terminal »[9]. The functioning of these technical devices is never described, only the actions they're allowed to be used for such as « listening or recording conversations or identifying or locating a person or a thing »[10] and the context in which they can be used are depicted.

On the Internet, leaked catalogues from companies that conceive, build and sell such devices inform a bit more on their nature. Indeed, they often detail on which kind of protocols or frequency bands they can be used (GSM, EGSM, GPRS, CDMA among others), as well as their coverage range, number of devices being monitored at once, action mode (active or passive), power requirement and/or autonomy (battery life), kind of interception (id, voice, text) and price. The pictures attached give and idea of their dimensions and portability. Similar information can be found on websites such as alibaba.com, giving more details about their dimensions and weight. If these sources accurately describe the object itself (from a product design perspective), it tells little about which flaws of the network they exploit (matter of industrial secret).

Lastly, the most important source of information for

remaking is actually be found from open source communities such as Osmocom (Open source mobile communications), OpenBTS and YateBTS who aim to substitute complex proprietary systems with open source software and tools and provide documentation and tutorials to build femto or picocell[11] sites in areas not covered by GSM networks. Also, independent programmers and hackers put online scripts to demonstrate the use of IMSI catchers and to rebuild them « to better understand the GSM infrastructure ». Those are the main sources of information that have been used to build the following prototypes

## 2. Remaking process

A way to face this lack of resources is to try to rebuild different versions of IMSI catchers. This remaking process can demonstrate what the technology really is and how it operates; it's also a manner to question the limits of the device to expose the misrepresentations around it and to test assumptions, in order to discuss its apocryphal character.

### A. Passive vs. active

IMSI catchers work on two different modes: a passive one and an active one. In the passive mode, the IMSI catcher doesn't "catch" International Mobile Subscriber Identities perse but monitors them instead. It "listens" to the ongoing broadcast network activity of a given cell tower and looks for plain text IMSIs (sent by the phones themselves when they connect with the cell tower) and doesn't interfere with this activity. A passive device works on a given area which is the area covered by the tower (which is in fact designated as the "cell"), the device will then get the identity of phones present in this cell.

In the active mode, the IMSI catcher replicates the activity of a cell site, it can spoof the identity of a regular cell tower, so the cellphones around associate themselves to it in total transparency for the user (it's a man-in-the-middle attack). An active device works locally on a given area which depends on its emitting power (the more powerful, the biggest the area). If it's not connected to the existing GSM infrastructure (local mode), it is not capable of passing outgoing phone calls or handling outgoing text messages, it is only capable of catching IMSIs of connected phones and of handling communications in between them. If it's connected to the existing GSM infrastructure (to a regular cell tower), it is capable of redirecting outgoing traffic, and by forcing unencrypted communication, it is able to intercept phone calls and text messages.

The IMSI is actually composed of the MCC (Mobile Country Code), the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number) (fig.1), in other words: the identifier of origin country (i.e 228 for Switzerland, 208 for France), the identifier of mobile network operator or carrier (i.e in Switzerland, 01 for Swisscom, 02 for Sunrise, 03 for Salt) and the identifier of the SIM card (associated to its user and a phone number).

fig.1 Example of an IMSI

### B. Two passive embodiments

The first version of a passive IMSI catcher that I rebuilt works with osmocomBB – a free and open source GSM software implementation running on a Ubuntu laptop and a compatible phone: in this case a Motorola C118, a 30$ phone that is programmable with a dedicated USB serial cable (fig.2). By running osmocom dedicated firmware on the handheld device, it is possible to tell it to accomplish specific tasks. In this case forcing the phone to listen to the broadcast traffic of a specific cell site. Decoding and filtering the incoming traffic allows to isolate the paging requests (when phones attempt to authenticate with the cell tower) which contain the IMSI of requesting phones in plain text (fig.3).

fig.2 Laptop, Motorola C118, USB serial cable

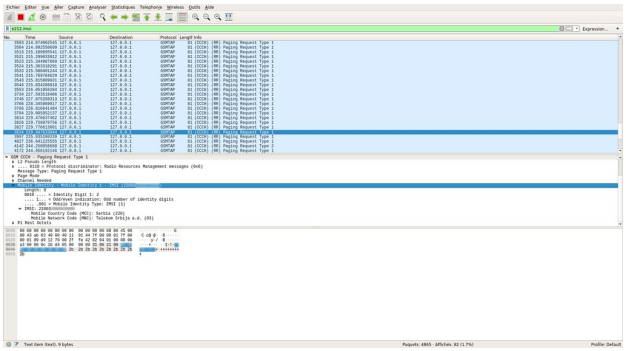

fig.3 Wireshark showing intercepted packets and IMSIs

The second version of a passive IMSI catcher that I rebuilt is based on a Realtek RTL2832U chipset, commonly found in DVB-T dongles, that are sold on the Internet around 10$ to watch television and a laptop running Ubuntu (fig.4). Using software-defined radio (SDR), it is possible to use this dongle to scan for GSM frequency bands. That is what the gr-gsm[12] software suite allows to do : 'grgsm_scanner' first scans the surrounding for GSM cell towers (fig.5) and 'grgsm_livemon' then listens to the specific frequency of the chosen cell tower (fig.6). The data acquired with grgsm_livemon is then interpreted with the help of the 'simple_IMSI-catcher.py' script provided by Oros42 on Github[13]. As in the previous setup with osmocomBB and the Motorola C118, the python script is looking for paging request which contains IMSIs in plain text (fig.7).

fig.4 Laptop, Realtek RTL2832U, antenna

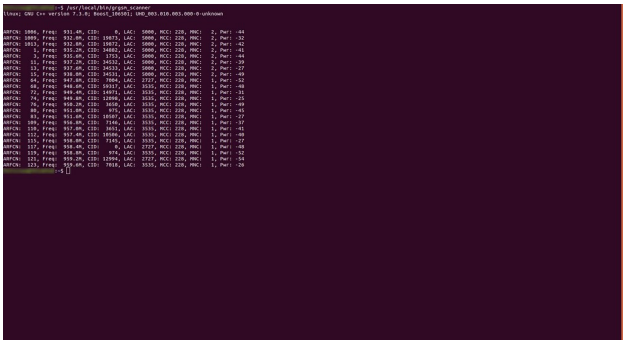

fig.5 grgsm_scanner

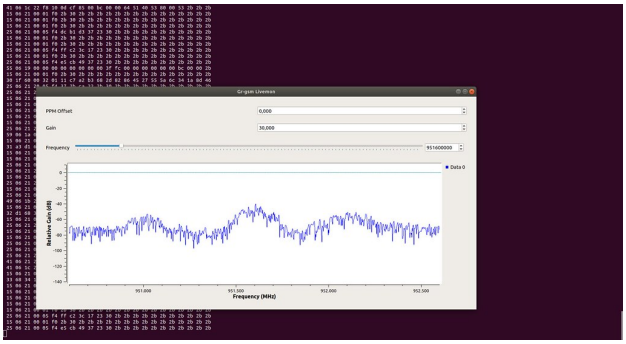

fig.6 grgsm_livemon

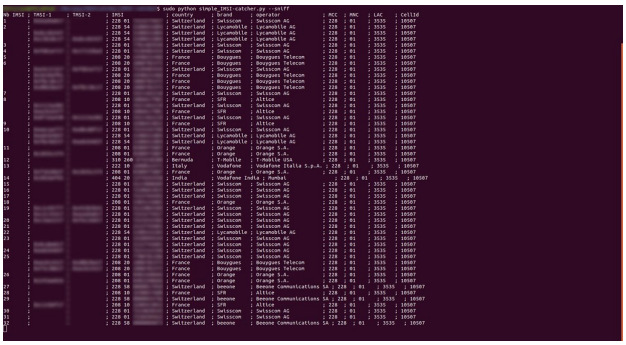

fig.7 Python script showing IMSIs in plain text

As their name suggests, while they are not able to

interfere with their environment, these passive devices are in a "listening" mode that can already tell a lot about their surroundings. Despite the use of encryption algorithms (namely A5/1 and A5/3) to protect the communications (phone calls, text messages), the IMSI is always transmitted in plain text in the air during the authentication process. As the IMSI is a unique id, those passive attacks provide enough information to discriminate and track a user in a given cell. From the MCC and MNC the script gives the origin country and operator of associated phone, it is then possible to get 'pictures' of different locations. For an example, the experiment has been conducted in two different locations: in Geneva, Switzerland which is a very cosmopolitan area (partly because of the international organisations) the devices gave IMSIs from various origins; in opposition, in Murmansk, Russia, the devices gave Russian IMSIs only.[14]

The previous devices are able to listen to one given frequency at a time, but it is feasible to set up multiple devices at the same time to obtain a multi-band sniffer.

### C. One example of an active device

To rebuild an active IMSI catcher one has to set up a fake base station; thus, cell phones in the surroundings think it is a legitimate/regular one and connect to it. In order to rebuild such an active device, I set up a bladeRF x115 (a full duplex SDR – that can transmit and receive at the same time) with YateBTS[15] (an open-source software implementation of GSM/GPRS radio access network) on a laptop running Ubuntu. YateBTS provides "Network in a PC" ("NiPC"), a local cell site that « performs all the functions of a regular GSM network », such as routing calls or handling SMS between local devices. NiPC allows you to set the frequency on which you emit but also other requirements for your network to work such as: MCC (Mobile Country Code), MNC (Mobile Network Code), LAC (Location Area Code) and CI (Cell ID)(fig.8).

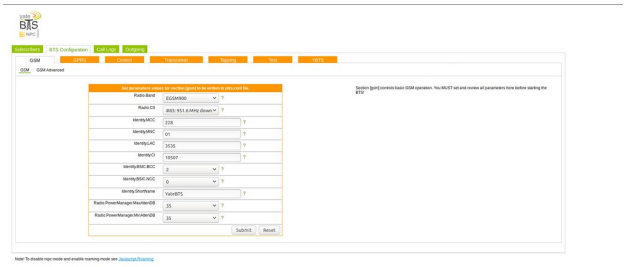

fig.8 Network in a PC web interface

While researching for this paper, I have implemented an off-the-network local cell site (not connected to the regular GSM infrastructure, mostly for legal reasons). This network was then only able to first get IMSIs of hooked phones, and then pass calls and handle messages in between phones associated with it (no outgoing communications). Though, by copying legitimate MCC, MNC, LAC and CI one can spoof the identity of an existing cell tower. By redirecting the traffic to the existing mobile phone network, without using any encryption algorithm (A5/0) in between mobile phones and the spoof cell tower, one can intercept communications such as phone calls and text message.

Nevertheless, some limits exist to this attack. First of all, the bladeRF x115 doesn't have a high emission power level, only nearby phones can be hooked. It is only 2G capable, and as Kenneth van Rijsbergen underlines it in his paper, a smartphone will rather stay on a weaker 3G/4G network than hook on a more powerful 2G network (Van Rijsbergen, 2016), consequently it is easier to target 2G phones. It constitutes an element which demonstrates that this apocryphal technology is not as effective as thought. Indeed it shows that attacks based on this particular hardware are not effective against recent smartphones. Nonetheless, remaking other versions on an IMSI catcher based on different hardware (e.g. more powerful) or targeting otherweaknesses of the network (e.g jamming 3G/4G frequencies so the phone downgrades to 2G) might show different results.

## 3. Relevance of remaking the present

Considering the relevance of remaking in Science and Technology Studies and Digital Humanities,

Sayers uses this kind of method to remake historical objects; for him these methods allow one to learn about « composition », « assembly », « interface », « failure », « abstraction », « instrumentalism » and « speculation » (Sayers, 2014). This approach is also relevant in the case of the IMSI catcher: though not being a historical object, it is a confidential one, and it is possible to draw a parallel with the lack of resources facing the remake of a historical object. For a historical object, some media can be missing: « Even if [media] cannot be fully recovered, prototyping puts pressure on these changes, opening them up to speculation » (Sayers, 2015); the same goes on for the IMSI catcher, as the sources of information can be incomplete, misleading or even non-existent. As Sayers adds about prototyping the past (Sayers, 2015), such prototypes are « tangible reminders of what was forgotten, ignored, destroyed, or lost », in the IMSI catcher case it would be « a tangible prototype of what is not accessible yet to everybody ». This « trial-and-error experimentation » allows one to test assumptions about the conception and production of the investigated technology.

In « Matters of Composition », Sayers addresses the question of materials needed to rebuild a historical artefact: « from what materials was it made? ». For him, it tackles interesting issues – not only around the composition of the object itself, but also around the sourcing of the materials and technological innovations in a given historical context. In the IMSI catcher case, I didn't rebuild the hardware exactly as it requires advanced skills in electronic and telecommunication engineering; I rather looked for and assembled off-the-shelf pieces of hardware such as laptop, radio interfaces and antennas. An interesting point, however, is that the off-the-shelf availability (in other words, on the public market) and the origin of a 30$ cell phone, a 10$ digital TV dongle and a dedicated 700$ wide band full duplex SDR card. Indeed, for the cheaper devices, one can easily order them on eBay and Chinese websites as they are not intended for the way this project used them. For the latter, it is a bit different as it must be (even briefly) stated in which country and for which reasons it's going to be used (being in an academic research context seemed to help to order the device). This raises the question of the legality of owning such devices, as the hardware pieces are not illegal to own, but using them to catch IMSIs is illegal.

In « Matters of Assembly », Sayers asks the question: « through what processes was it made? ». For him, « an interest in process is often an interest in what cannot be recovered from the historical materials at hand » ; in our case it is an interest in what is not available from public sources. Indeed, the attempts to reassemble an IMSI catcher were first based on pictorial elements, such as photographs of existing IMSI catcher in leaked catalogues (in which you can find several shapes of objects ranging from handheld devices to black boxes the size of an electrical cabinet), or on retailing websites such as Alibaba. Apart from the different shapes and the nature of a few components of the devices these images doesn't inform on the way it operates. As it has been said earlier, the main source of information is found from open-source communities that provide abundant documentation to rebuild IMSI catchers « to better understand the GSM infrastructure », or to build femto or pico cell sites in areas not covered by GSM networks. In this way, trying to better understand the processes (or the weaknesses) the IMSI catcher relies on was a manner of addressing its nature and discussing its apocryphal character; if we put it through Sayers framework: « does the IMSI catcher work as thought? does it work at all? ». This raises the question of (mis)representations of apocryphal technologies and the way they really operate; remaking a few versions of IMSI catchers allowed us to better understand these operating processes and to expose potential limits to the devices that are actually not working as thought by the public. Finally, in Sayers' historical approach « these questions frame technologies as processes, not products frozen in time. » ; which is also relevant in the case of the IMSI catcher, as it is a contemporary and still evolving object.

In « Matters of Interface » Sayers discusses in what types of interactions the object was made, used or circulated. In the IMSI catcher case, the interface has very little documentation or none at all, as it is a secret object, that is known to be used but never in front of the public. Nevertheless, it makes some appearances on public budgets.[16] These budgets give the name of the companies selling the devices and their price. Also, some documentation exists in the form of laws and

its use has been reported in different contexts (e.g. as an industrial spying tool in India[17] (Parks, 2016)). This raises some questions such as the automation of these devices and the technical level required to use them or if they actually need an operator at all. While the remaking allows one to learn about interfaces in open-source communities, and that it is possible to automate them with some scripts; it is, however, nearly impossible to answer these questions from the government side. Indeed, it is not possible in our case to affirm that governmental IMSI catchers rely on the same hardware, hence it is impossible to draw precise conclusions about their use; but it opens up to speculation, which does not help in the idea of unveiling the apocryphal aspect of the technology. This shows some limits of the remaking process in order to answer specific questions.

« Matters of Failure » tackles the question of the success of an object. It is almost impossible to assess the success of the IMSI catcher from the available documentation. If it is already hard enough to find relevant information about working IMSI catchers, then sources of information about discarded devices certainly don't exist. Nonetheless, the process of remaking induced a « trial and error » process and also shed light on a multiplicity of objects operating in different ways under the same name, which implies that different versions coexist probably with their own efficiency or « success » among the services using them.

In « Matters of Abstraction » Sayers asks the question : « Through what media was it expressed, and how? » which in our case refers to the questions of sources and documentation of the devices. As it has been said before, while leaked catalogues give a visual representation and sometimes dimensions of the devices, open-source communities give us software (under the form of source code) to rebuild them. It is the articulation of these multiple sources that enable the reconstitution of the device and that allows to explore its nature and operating processes. As Sayers writes, « Each of these arguments abstracts multiple dimensions, positions, and perspectives, translating the relations between them into something communicable, interpretable, and archivable (e.g., the official record). Remaking a device is haunted by abstracted relations, reminding us that we cannot fully recuperate embodied processes while giving us a granular sense of what those processes might have entailed. » Then, it is possible to show what an IMSI catcher actually looks like and how it works only if we take care of articulating the different sources of information we have at hand.

« Matters of Instrumentalism » raises the question of documentation of the process and remade devices. In the very particular case of the IMSI catcher, the aim of the research is not to write a manual to build the most effective device but rather to, first, explore its nature and its apocryphal character, and then, to get enough material to carry on further research steps. As I am approaching this research from a design and practice-based perspective, the results of this reconstitution will be shown in incoming exhibitions.

The last point Sayers makes about the relevance of remaking is « Matters of Speculation ». In the historical approach it concerns what is not known, what is not at hand. These two questions are obviously at the core of the research when tackling a confidential or apocryphal technology. From an historical concern, when the documentation is not available, part of the reconstitution has to be speculated. Thus, the researchers are « building and testing a variety of possibilities, comparing them with what was available or popular at the time, and determining what's feasible for circulation. ». This is what I have partly made by testing different iterations of IMSI catchers, but it will be developed further in the research by prototyping potential existing IMSI catchers derived from the ones presented earlier (with different factors of autonomy, mobility, or networking).

**4. Myths and speculation**

There is an inherent speculative aspect when approaching apocryphal technologies. As stated previously, speculation is needed when one does not have the resources at hand, what is not known has to be speculated. But dealing with such an apocryphal technology offers another space for speculation: the space for what is to come (speculative futures), or what could have been (alternative presents), which might be the most interesting part in the research process in a design fiction perspective.

In that sense, the idea behind debunking the myth with the '(reverse) engineering' approach is not to replace a representation by another, as it would raise other concerns and myths. It is not an end in itself, but should rather be seen as a step to open a whole new space of speculation. This can be done by drawing what Yves Deforge calls « technical lines » (fig.9)(Deforge, 1985), obtained by studying and identifying the existing forms of an IMSI catcher, lying on the notions of principle, function and evolution. Then, by inferring from theses existing forms and from weak signals (e.g. drone embedded devices, wearable prototypes) it is possible to infer 'yet-to-come' devices. If this design fiction approach allows to get rid of technical and technological constraints it is important to keep in mind the realities of existing objects. The remaking of one or several IMSI catchers gives a basis to better understand the technology, which is a starting point for « crafting the speculation » (Auger, 2013). Indeed as Auger argues, basing visions on « logical trajectories » or « the rules of real life » allows « to craft the speculation into something more poignant, based on logical iterations of an emerging technology and tailored to the complex and subtle requirements of an identified audience. » In the case of the IMSI catcher, this allows one to overcome its apocryphal nature in order to come up with « alternative presents and speculative futures » (fig.10)(Auger, 2013). Speculative scenarios about the technology raise tension points to start a more global reflection about legitimacy and ethics in the deployment of such surveillance systems. Then, designing iterations about speculative futures or alternative presents of the IMSI catcher give the ability to reflect on its consequences in the present and critique its current use.

As an example, I recently used the two passive devices previously described in an audiovisual performance[18] showing the space the GSM infrastructure takes in the city and the IMSI and origin of phones flowing in the nearby neighborhoods. This performance raised many reactions from the audience expressing their concerns and speculating about how this technology is used by law enforcement and its limits regarding privacy.

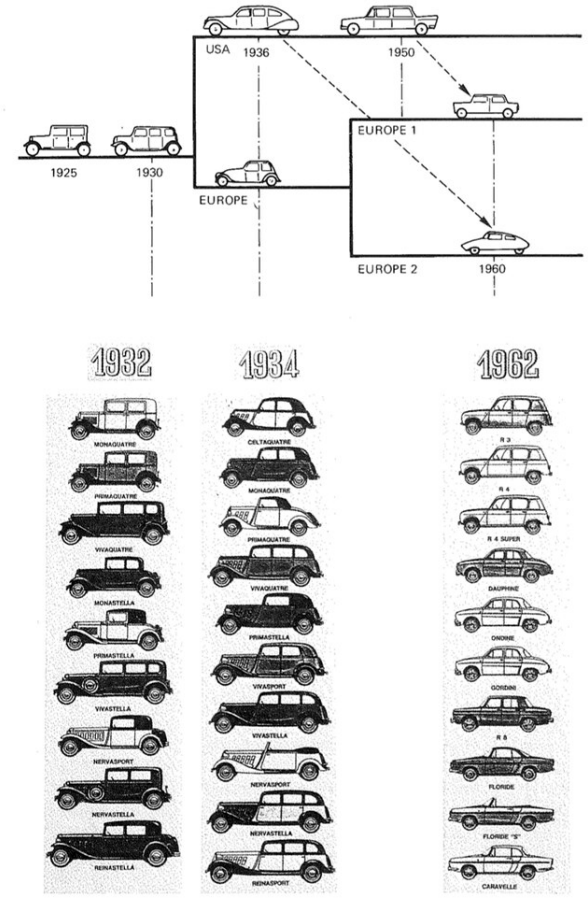


fig.9 Yves Deforge. Technologie et ge□ne□tique de l'objet industriel. 1985. p.121

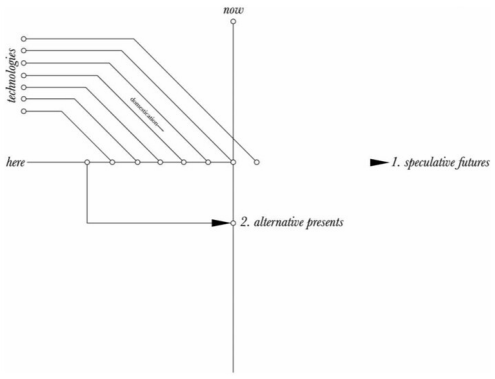


fig.10 James Auger. « Alternative presents and speculative futures ». 2012

## 5. Conclusion

In this paper, we saw that it was possible to deal with the apocryphal character of a technology with a practice-based remaking process. The reconstitution of three different versions of IMSI

catchers allowed to challenge the lack of documentation. By using off-the-shelf hardware and open-source software, it is possible to re-create similar devices to explore and learn about its functioning and the environment it relies on. Using remaking methods allows to re-appropriate the technology, but also to show its limits and the dependencies it has with its environment. In this way, the process of remaking embodiments of such a technology allows to discuss its apocryphal character. As we saw, it doesn't work as well as thought and it shows some limits in its range of use and the type of phones concerned by this kind of attacks.

Compared to Sayers approach for historical objects, we also discussed the relevance of remaking when dealing with a contemporary object. This trial-and-error approach allows to face the confidential character of a present technology as it allows one to face the lack of documentation of a past technology, it allows one to answer questions about the way it works or the way it is supposed to work.

Nevertheless, there are obvious limits to such a methodology. Indeed, the hardware used here does not meet the technical specifications of the one used by governments or intelligence agencies: the means used to lead this research are not dedicated to surveillance, it is rather a hijack of their primary use. Thus, it is only possible to speculate about the exact functionalities and use of devices own by intelligence agencies. The whole process is then a kind of approximation that unveils only a bit of the mystery around such surveillance devices.

Finally, the results presented here constitute an abundant toolbox to broaden the research about a larger field in the context of surveillance, we could probably use the same kind of methods for other objects of the surveillance to explore their true nature and effects. It is also toolbox to examine other characteristics of the object such as its own concretization process, and its effects on its associated milieu (Simondon, 1958); in that, it is a basis for speculation and to imagine technical lines of future devices.

---

[1] IMSI stands for "International Mobile Subscriber Identity", a unique number associated to a SIM card

[2] <https://en.wikipedia.org/wiki/Man-in-the-middle_attack>. Accessed: 2019.03.01.

[3] < https://www.lemonde.fr/pixels/article/2015/05/20/les-douanes-ont-achete-des-imsi-catchers-alors-que-leur-utilisation-est-illegale_4636988_4408996.html >. Accessed: 2019.03.01.

[4] Although exposing some hacking methods and being based on open source software, this paper is not a technical reference about how GSM networks operate or a how-to re-create an IMSI catcher. It's rather a way of arguing the relevance of rebuilding a confidential object to discuss its apocryphal character. Hence, some approximations can be found even if the author tries to be the more precise possible.

[5] <http://www.businessinsider.fr/us/mysterious-fake-cellphone-towers-intercept-calls-2014-9>. Accessed: 2019.03.01.

[6] < https://www.bbc.com/news/technology-43639709 >. Accessed: 2019.03.01.

[7] « dispositifs techniques spéciaux de surveillance de la correspondance par télécommunication » Art. 269bis1 of Code de procédure pénale suisse du 5 octobre 2007

[8] « dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet » Art. L. 851-5. LOI n° 2015-912 du 24 juillet 2015 relative au renseignement

[9] « utilisation d'un appareil ou d'un dispositif technique […] afin d'intercepter des correspondances émises ou reçues par un équipement terminal » Art. L. 852-1.-II. LOI n° 2015-912 du 24 juillet 2015 relative au renseignement

[10] « d'écouter ou d'enregistrer des conversations, ou d'identifier ou de localiser une personne ou une chose » Art. 269bis1 of Code de procédure pénale suisse du 5 octobre 2007

[11] small cellular base station covering a small area

[12] https://github.com/ptrkrysik/gr-gsm. Accessed: 2019.03.01.

[13] https://github.com/Oros42/IMSI-catcher. Accessed: 2019.03.01.

[14] The author works and conducts his research in Geneva. The experiment in Murmansk has been conducted during a performative lecture for Inversia on February 9, 2019.

[15] BTS stands for base transceiver station

[16] < http://www.douane.gouv.fr/Portals/0/fichiers/datadouane/marches-publics/2014-marches-publics.ods>

[17] < https://www.dailymail.co.uk/indiahome/indianews/article-2239422/Government-hunts-elusive-bug-DoT-wants-snooping-listening-devices-private-sector-surrendered.html>

[18] Félicien Goguey, 900 MHz, live performed at Musée d'ethnographie de Genève, May 2019.

**REFERENCES**

[1] Allen, Jamie. « Apocryphal Technologies (special issue) », call for papers in continent., 2018.

[2] Auger, James. « Speculative design: crafting the speculation » in Digital Creativity, Volume 24, 2013 - Issue 1. 11-35

[3] Deforge, Yves. Technologie et ge□ne□tique de l'objet industriel. Paris : Maloine, 1985.

[4] Farman, Jason. « Surveillance from the Middle, On Interception, Infrastructure, and the Material Flows of Asynchronous Communication », in Media Fields Journal n°11, 2016.

[5] Parks, Lisa. « Technostruggles and the Satellite Dish: A Populist Approach to Infrastructure » in Cultural Technologies: The Shaping of Culture in Media and Society. ed. Göran Bolin, New York and London: Routledge, 2012.

[6] Parks, Lisa. « Rise of the IMSI Catcher » in Media Fields Journal n°11, 2016.

[7] Sayers, Jentery. « The relevance of remaking », Maker Lab in the Humanities. Victoria, BC: University of Victoria, 2014. . Accessed: 2019.03.01.

[8] Sayers, Jentery. « Prototyping the Past » in Visible Language 49.3, Critical Making, Design and the Digital Humanities, 2015.Simondon, Gilbert. Du mode d'existence des objets techniques. Paris: E□ditions Aubier, 1958.

[9] Strobel, Daehyun. IMSI Catcher. Ruhr-Universität Bochum, 13.Juli 2007.

[10] Van Rijsbergen, Kenneth. The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF. University of Amsterdam, 2016.