**What electronic warfare can learn from a wagon full of smartphones**

By: [Kelsey D. Atherton](https://www.c4isrnet.com/author/kelsey-atherton)   6 Feb 2020

<https://www.c4isrnet.com/battlefield-tech/2020/02/06/what-electronic-warfare-can-learn-from-a-wagon-full-of-smart-phones/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2002.06.20&utm_term=Editorial%20-%20Early%20Bird%20Brief>

****

*Normally creating a traffic jam takes actual traffic, like the cars seen here. With a wagon full of smartphones, a traffic jam can be created without the need for a long line of cars. (EveryPicture, via Wikimedia Commons CC-BY-SA-3.0)*

A single red wagon, hand pulled down the middle of a lightly traveled street, is an odd delivery mechanism for an electronic warfare attack.

It is only slightly less unusual as a kind of art exhibit. But the wagon’s payload, and its artist brush, is the same: 99 second-hand smartphones, all opened to Google Maps.

In a simple demonstration, Berlin-based artist Simon Weckert rolled the wagon full of phones through several streets and, in so doing, created virtual traffic jams as Google Maps interpreted the phones as slow-moving cars. Screen captures of the demonstration, paired with video from the street, show the traffic mapper interpreting the wagon phones as first nothing, then as a slowdown, and then in a deep red line painted over the virtual road, as a rush hour-esque standstill.

It is not that often that a Berlin digital arts experiment has lessons for electronic warfare and digital manipulation, but with the greater proliferation of virtual environments its worth pulling a few principles from this wagon of tricks.

First: identify how the default use of a system can be actively gamed.

Basing traffic density algorithms on the number of smartphones geolocated to a path along a street is, by and large, an effective short-hand for mapping traffic density in an era where cars themselves do not broadcast their location. Faking traffic, as done in real life by Weckert here or as explored within the code of the navigation apps as with this [Waze demonstration from 2014](https://www.popsci.com/article/gadgets/israeli-students-spoof-waze-app-fake-traffic-jam/), is a risk, but one that mostly requires deliberate action, and which can be checked against in-person observation, if needed.

Second: virtual hacks mostly cause real-life obstacles for people who rely on them.

Without having been in Berlin as Weckert rolled his wagon down the street, it’s hard to conclusively say what effect the virtual traffic jam had. For people already on the road, the new route information may have redirected them elsewhere, but only if they were also using a traffic-navigation aide.Top of Form

As the military adopts tools like ATAK, the Android Team Awareness Kit, for tracking and coordinating movement in a virtual environment, planners and commanders should be aware of the possibility that additional, misleading information is pumped into the same system. Hiding the location of a formation of troops, or creating a false impression of a team in a vital overwatch position, are ways a spoofed virtual environment could lead to disaster.

Third: the existence of tracking data from commercial smart devices is only going to complicate the future.

Weckert’s demonstration used phones to simulate cars in a civilian street. That alone could be a means for forcing a reroute of a target and laying an ambush, should a malicious actor decide to do so. (And if Google doesn’t respond to mitigate how the map hack worked.) In a future where infantry carry personnel trackers, spoofed Fitbits attached to a drone could allow an adversary to create a false impression of peril far from where they want to act, pulling needed resources away from a fight on a virtual snipe chase.

Because virtual environments are used in real-time to understand and interpret the world, manipulating effects in a virtual space can spill over to real-world consequences.