Chapter 25
Measuring the World:
How the Smartphone Industry Impacts Cyber Deterrence Credibility

Dirk Westhoff
University of Applied Sciences Offenburg, Germany

Maximilian Zeiser
University of Applied Sciences Offenburg, Germany

ABSTRACT

The authors claim that location information of stationary ICT components can never be unclassified. They describe how swarm-mapping (crowd sourcing) is used by Apple and Google to worldwide harvest geo-location information on wireless access points and mobile telecommunication systems' base stations to build up gigantic databases with very exclusive access rights. After having highlighted the known technical facts, in the speculative part of this article, the authors argue how this may impact cyber deterrence strategies of states and alliances understanding the cyberspace as another domain of geostrategic relevance. The states and alliances spectrum of activities due to the potential existence of such databases may range from geopolitical negotiations by institutions understanding international affairs as their core business, mitigation approaches at a technical level, over means of cyber deterrence-by-retaliation.

1. INTRODUCTION

1.1. Background

In 2012 Barack Obama commanded his senior national security and intelligence officials to draw up a list of potential military destinations of the cyberspace, to develop means to mitigate their proper functionality as well as to develop means to destroy these destinations. According to the Guardian the Presidential Policy Directive 20, issued in October 2012 but never published, states that what it calls Offensive Cyber Effects Operations (OCEO) "…can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging…" (The Guardian, 2012).

DOI: 10.4018/978-1-5225-7909-0.ch025

It would be interesting to understand if this objective from a NATO founder member respectively a member of the United Nations Security Council is yet in line with the recent reconceptualization of NATO's cyber deterrence thinking, namely "…that deterrence should be understood as a cumulative process of ongoing offensive and defensive operations that repeatedly demonstrate intent and capability as a means of generating credibility…" (Pijnenburg Muller & Stevens, 2017).

This article investigates whether one has to consider smartphones as a potential Swiss Army knife to provide useful geostrategic information with respect to the information cyber warfare. If that is the case it would prove another example for the multiplicity interdependencies of state, FAMGA[1] and other tech companies in this arena. As publicly known since Snowden (Greenwald, 2014), the NSA holds various strategic partnerships, namely alliances with more than 80 private companies according to the Special Sources Operation (SSO)-program.

The contribution of this article is in line with the work from Jøsang (Jøsang, 2014) discussing potential cyber-war capabilities of major technology vendors. However, in this work the authors zoom to a specific but global scenario. The authors want to draw the attention to the mobile digital device market's potential impact on cyber deterrence due to information infrastructure warfare, or, more concretely, what has been coined swarm mapping. Besides others it has also been pointed out in (van Niekerk & Maharaj, 2010) that "…the mobile infrastructure is important for national wellbeing, and should be explicitly considered as part of the critical information infrastructure." In the rest of this article authors consider mobile devices running iOS or Android. This class of digital devices together with the movement patterns of citizens are ideal for measuring the digital world's wireless entry points as explained in this article. The title is chosen in similarity to the book title *Die Vermessung der Welt* (Kehlmann, 2005).

1.2. User Behavior and Worldwide Mobile Device Penetration

Let us hypothetically answer the following question. If someone you do not even know hands over a digital device to you and asks: "Would you be so kind travelling for me in your homeland or any other foreign country and spy out the remote surrounding as much as you can? And by the way, we also want to get an idea about you and your personal behavior respectively interests and plans. Maybe we would also like to know what people you met and at what time and at which various places you paused for what exact duration."

How many people would agree on that deal? 1%, 2%, probably 5%, but definitively not more. We all do know better: Only during the last quarter of 2016 more than 400 million people bought a smartphone (only Android or iOS) worldwide. This gives an impression on the huge number of proud Android and iOS smartphone users typically keenly searching for connections, having continuously activated WLAN, Bluetooth and GSM/UMTS and moving from one place to the other, either on foot, car, or train. Not even counting tablet users of other portable Android devices like digital cameras, etc. One may argue that according to some study 'only' 67% of the users apply Apps with access to location-function (Goldmedia 2014). Nevertheless, this is still a huge amount of devices which surely serve an appropriate penetration for the below described scenario. However, for iOS it simply doesn't matter whether the user has decided to disable location based services or not. Moreover, for iOS 11 (available in September 2017) but also Samsung's Galaxy S8 the user cannot such easily disconnect from WLAN and Bluetooth anymore. Even if this disconnects the actual connection, the modules itself are still sending and receiving beacons and are enabled to read Received Signaling Strength Indication (RSSI) values and others. In consequence, even with WLAN and Bluetooth OFF, the below described approaches still work.