

The Invisible Digital Beacon: How Our Smart Devices are Redefining the Battlefield (and Privacy)

We are used to thinking of cybersecurity as a war involving Russian or Chinese hackers attempting to breach government firewalls. But the reality is much more mundane, and for that reason, more unsettling: the greatest flaw in national security systems is not obsolete software, but the watch on your wrist or the app that counts your steps.

By Dr. Gustavo Scotti di Uccio – AOS PGD¹



The Trojan Horse in Your Pocket

In the world of defense, it is called OPSEC (Operational Security), the discipline that denies adversaries crucial information about one's capabilities and intentions. For decades, OPSEC meant not talking at bars, not photographing documents, and encrypting radio communications. Today, in the era of hyper-connectivity, the paradigm has shifted. Every soldier, official, or ordinary citizen has become a mobile sensor transmitting data in real-time.

The problem does not necessarily lie in a targeted external attack. The real "bug" is the Human Factor. Driven by the desire to monitor our athletic performance or stay connected with family, we voluntarily feed the network with sensitive data. Smartphones, smartwatches, and fitness trackers are designed for "perennial connectivity," unintentionally turning into beacons that signal secret locations and tactical movements.

When "Big Data" Becomes a Weapon: The Strava Case and Beyond

The most striking case dates back to 2018, when the fitness app Strava published a global "Heat Map" of its users' activities. The intent was purely statistical and promotional: to show where the world runs and cycles. However, in war theaters such as Syria, Afghanistan, or Niger—where civilian use of such technology is almost non-existent—the map revealed the exact layout of secret U.S. and French bases.

The "luminous trails" created by soldiers running around the perimeter of the base allowed analysts to identify patrol routes and logistical zones with surgical precision.

This is not an isolated incident. An investigation into Polar Flow showed it was possible to trace the identities, names, and even home addresses of NSA agents and British secret service members simply by cross-referencing public data from their training sessions. If an agent habitually runs around an anonymous building in Fort Meade and then returns home to a Washington suburb, the game is up: anonymity is compromised.

The Metadata Trap: The Ukrainian Front

The war in Ukraine is offering a brutal lesson on the use of social media in combat. Many soldiers, often very young, upload videos to TikTok or Telegram to show life at the front. Even without activating geolocation, EXIF metadata (hidden information in image files

¹ AOS is an Independent company registered in Belgium since 2012. It delivers technical, engineering, operational and management support for defence and security sector at national, European & transatlantic levels. In systems engineering & programme management for the development of complex & innovative projects. In last 5 years, AOS has carried out more than 80 NATO studies and EU projects in interoperability, emerging technologies, air defence, energy management, UAVs, & dual-use solutions. AOS team consists of senior managers & engineers from Belgium, the Cz. Rep., France, Germany, Italy, Luxembourg, Portugal & Spain with extensive experience in defence industries, Ministries of Defence, and EU institutions

including date, time, and GPS coordinates) or simple geographical references in the background (a high-voltage tower, the shape of a hill) allow OSINT (Open Source Intelligence) analysts to provide exact coordinates for drone or artillery attacks within minutes.

The Science of "Pattern of Life"

Enemy intelligence today doesn't need to peer through windows. It uses SIGINT (Signals Intelligence) and "Big Data" analysis to study the so-called **Pattern of Life**. By aggregating hundreds of seemingly harmless GPS tracks, it is possible to determine:

- **Critical Times:** At what time does the guard change occur?
- **Logistics:** What are the preferred routes for supplies?
- **Hierarchies:** Who is the individual moving most frequently between the command center and living quarters?

This is not just theory: the precision of civilian GPS (5-10 meters) is more than enough to program a targeted attack or for Social **Engineering** attempts (blackmail or forced recruitment) based on a target's personal habits.

Awareness and Digital Hygiene: Defense Starts with Us

How can we protect ourselves in a world where "every signal is a target"? The answer is not just technological, but cultural.

- **No-Device Zones:** Inside sensitive areas, the use of any Bluetooth or Wi-Fi device must be prohibited.
- **Faraday Bags:** The use of shielded pouches that block every electromagnetic signal during transit to classified sites.
- **Cyber-Hygiene:** It is essential to configure social and fitness profiles as "Private," disabling location services by default.

The Paradox of Convenience

The challenge of the future is understanding that the convenience of smart technology is inversely proportional to our security. Every time we accept an app's terms of service without reading, or upload a selfie "tagging"

our location, we are surrendering a piece of our digital sovereignty.

Reflections for the Future

Military and government personnel today represent only the vanguard of a problem that, in reality, concerns everyone. If a simple smartwatch can compromise an international mission, the same device is capable of exposing the details of our private lives to malicious actors or unscrupulous companies. This vulnerability is not confined to war theaters: in our daily lives, every hurried acceptance of an app's terms of service or every geographical "tag" on social media represents a conscious surrender of a fragment of our digital sovereignty.

As early as 2023, a U.S. Department of Defense (DoD) report sent to Congress in July of that year, titled *"Use of Fitness Wearables to Measure and Promote Readiness,"* analysed the massive integration of smartwatches (such as Garmin and Oura rings) to monitor the health and operational readiness of soldiers, while also evaluating certain critical issues. Other academic studies and policy briefs from the **NATO CCDCOE** (Cooperative Cyber Defence Centre of Excellence) confirm that over 60% of global military personnel regularly use wearable devices during service. This widespread use among troops reflects a global trend in civil society, where the need for health monitoring often prevails over operational prudence.

The modern challenge lies in understanding that the convenience offered by smart technology is often inversely proportional to our security. Digital awareness must become an integral part of our daily "training" for connected life. It is no longer enough to build barriers against external attacks; the decisive step is **learning not to be the primary informants for those who wish to monitor or strike us**. In a hyper-connected world, digital discretion can no longer be considered an optional luxury, but must become a true survival strategy. The challenge—not only for institutions but for everyone—becomes balancing one's own well-being or that of employees with the vital necessity of remaining invisible to "enemy radars".