P | I | P | S

The Geointelligence Revolution

Real-Time Reconnaissance and Its Dangers

PIPS White Paper 10.5: *Executive Summary*

Alexander Nocks, Research Fellow
Sophie Glenn, Research Intern

Publicly available geospatial information and aerial imagery have many productive applications but are also increasingly satisfying the reconnaissance needs of terrorist organizations and other non-state actors. In the next five to ten years, reconnaissance that once required risky, time-intensive, in-person investigation will be carried out instantaneously and remotely. This real-time remote reconnaissance is less expensive, harder to detect, and faster than traditional reconnaissance methods.

Current U.S. policy restricts the type of aerial imagery available to the public but fails to mitigate the full scope of the growing threat. This paper proposes domestic and multilateral sales-tracking strategies to detect potential attacks without sacrificing the many benefits of widespread access to geospatial information and aerial imagery.

The Dual-Use Dilemma of Geospatial Intelligence

Geospatial intelligence (GEOINT) is the process of deriving intelligence from geospatial information and aerial imagery. When analyzed, these inputs provide significant situational awareness by allowing remote actors to describe, assess, and model physical features and geographically referenced activities.

The public GEOINT field is growing as individuals, businesses, non-governmental organizations, and the U.S. government take advantage of emerging GEOINT inputs and analysis abilities. These actors, including the National Geospatial-Intelligence Agency, are working to improve public GEOINT capabilities. Further, the clear profitability of collecting, analyzing, and distributing GEOINT inputs is leading more organizations to enter the public GEOINT market

There is an inherent tension between the constructive and destructive applications of GEOINT. This dual-use dilemma—in which the same information can be used to advance conflicting ends—has gone largely unaddressed by the policy community. Since low-level GEOINT currently available to the public introduces relatively few national security risks, the benefits of public GEOINT have overshadowed its dangers. Mapping storm damage saves the lives of evacuees—

but it may also direct looters to vulnerable areas. Improvements in public GEOINT capabilities will enhance both sides of the dual-use dilemma.

Current Threat Assessment: Low-Grade Public Geospatial Intelligence

Although current public GEOINT capabilities rely on outdated aerial imagery and sporadic geospatial information, internet reconnaissance has become commonplace in attack cycles. Criminal networks, terrorist organizations, and other non-state actors have been quick to adopt low-grade public GEOINT capabilities, primarily in the form of Google Earth and geotagging on social media.

Improving Public Geospatial Intelligence

Today, demand for enhanced public GEOINT abilities drives technological developments that will increase the volume, granularity, and temporal resolution of publicly available GEOINT inputs. Expanding mobile device usage and internet connectivity, along with emergence of the internet of things, allows more real-time geospatial information to be collected at a more granular level. Simultaneously, with remote sensing technology becoming more affordable, smaller, and easier to produce, many companies are entering the aerial imagery market. They will soon offer the public high spatio-temporal resolution coverage of much of the planet.

Data brokerage and aerial imagery analysis companies make high-level GEOINT capabilities publicly accessible. Without their involvement, many of the anticipated uses of public GEOINT would be impossible.

New Threat: Real-Time Remote Reconnaissance

As public GEOINT offers closer to real-time insights, it will shift from complementing in-person reconnaissance to offering superior insights—not only for target selection and attack planning, but also for attack execution. The next phase of public GEOINT abilities is real-time remote reconnaissance, in which potential adversaries can remotely conduct all surveillance required to prepare for an attack. It allows central agents to easily conduct reconnaissance, planning attacks without exposing themselves to detection.

Combining local-level knowledge with aerial surveillance allows potential adversaries to see around physical obstacles and gain enhanced situational awareness throughout three general phases of the attack cycle.

- *Target Selection*. Improved public GEOINT abilities expose vulnerabilities that would otherwise be difficult to detect. Revealing the physical environment, defensive structures,

and security operations surrounding a potential target also facilitates sophisticated target selection.

- *Attack Planning*. Real-time remote reconnaissance informs attack planning more effectively than either on-site reconnaissance or asynchronous remote reconnaissance. Visualizing the minutia of an operating environment enables attackers to prepare escape routes, plan for contingencies, and otherwise develop knowledge approaching that of a local.

- *Attack Execution*. By showing attackers and their handlers where responders, victims, and other entities are as an attack unfolds, real-time remote reconnaissance will provide attackers unprecedented situational awareness. Knowing how the environment is changing will help assailants inflict greater damage and escape more easily.

Shortcomings of Prior Restraint Policy

Current policy—known as prior restraint—seeks to mitigate the dangers of public GEOINT by denying some users access to certain subsets of satellite imagery. Statutory restrictions limit the spatial resolution of satellite imagery, prohibit collection on select sensitive sites, and prohibit sales of satellite imagery to certain buyers.

Meaningful prior restraint is becoming unachievable for three primary reasons.

- *Significant Costs to Other Users.* Denying access to GEOINT inputs hurts the many humanitarian, social, and commercial enterprises that also rely on public GEOINT. As access to real-time satellite imagery becomes the norm, attempts to delay the release of certain images may undercut their usefulness.

- *Alternatives to Regulated Satellite Imagery*. Foreign entities provide satellite imagery that is banned in the United States. While many top satellite imagery companies are currently U.S.-based, the market is going global. Furthermore, geospatial information and aerial imagery from UAVs reveal the same vulnerabilities as would satellite imagery. Reducing the quality of satellite imagery has little effect when the same information can be readily acquired elsewhere.

- *Undermines U.S. Satellite Imagery Market.* Requiring U.S. companies to degrade their satellite imagery reduces their ability to compete and creates a profit-incentive for companies to move overseas where the U.S. has less regulatory control. Restrictions that drive U.S. companies to leave makes prior restraint a self-defeating policy.

Data restrictions undercut the many constructive uses of satellite imagery, fail to deny potential adversaries significant GEOINT insights, and drive satellite imagery companies overseas. Prior

restraint and other blanket GEOINT denial programs are too clumsy for the future public GEOINT market. They undermine too many benefits, while failing to address too many dangers.

Counter-GEOINT Solution

The challenge of regulating dual-use information is balancing its constructive and destructive potential. However, the high risks of public GEOINT do not necessarily mean that they outweigh the benefits. Instead of denying all users access, the United States should pursue strategies to mitigate the risks, while maintaining the benefits of public GEOINT.

Three general strategies can best lessen the risks from public GEOINT without undermining its benefits.

- *Precise Restrictions.* For highly-sensitive sites—such as military bases—the destructive potential of sharing GEOINT inputs outweighs its benefits. Those facilities can best be protected by denying any form of surveillance. Imposing legal shutter control on domestic companies and checkbook shutter control on foreign companies can minimize the dangerous aerial imagery available. These sites should also block location tracking on their premises by prohibiting location information sharing on their grounds and using jammers to make location tracking impossible.

- *Mandatory Reporting.* All U.S. companies should be required to report the sale of geospatial information, aerial imagery, or GEOINT analysis. By collecting buyer and data subject information, the United States can detect remote reconnaissance as it happens. Since many companies offer specialized data and analysis, the best reconnaissance will likely include multiple purchases from different companies. Aggregating purchase data will reveal where reconnaissance is being targeted. Analyzing those patterns can expose potential plots and establish investigation targets, thereby allowing attacks to be detected before they occur.

- *International GEOINT Agreement.* While most public GEOINT is currently facilitated by U.S. companies, GEOINT organizations are proliferating worldwide. To ensure continued security as the market diversifies beyond the reach of U.S. regulations, the United States should work with the international community to coordinate policies for selling GEOINT inputs. Doing so will create a more comprehensive and reliable monitoring network, enabling plots to be detected even when potential adversaries buy GEOINT products from companies in different countries.

By adopting counter-GEOINT monitoring practices and encouraging their standardization worldwide, the United States can maximize the utility and mitigate the dangers of improving public GEOINT.