The West Has Forgotten How to Keep Secrets

By Jan Kallberg

August 8, 2022

Russian military planners now have access to a treasure trove of European data which can be used to circumvent Western defenses.

Open Source Intelligence (OSINT) has had an extraordinary moment in the spotlight thanks to Russia's invasion of Ukraine. Viewers have been able to see the effects of antitank weapons and the dreadful realities of war in close to real-time.

But OSINT, like all other intelligence, cuts both ways — we look at the Russians, and the Russians look at us. But their interest is almost certainly in freely available material that's far from televisual — the information a Russian war planner can now use from European Union (EU) states goes far, far beyond what Europe's well-motivated but slightly innocent data-producing agencies likely realize.

Seen alone, the data from environmental and building permits, road maintenance, forestry data on terrain obstacles, and agricultural data on ground water saturation are innocent. But when combined as aggregated intelligence, it is powerful and can be deeply damaging to Western countries.

Democracy dies in the dark, and transparency supports democratic governance. The EU and its member states have legally binding comprehensive initiatives to release data and information from all levels of government in pursuit of democratic accountability. This increasing European release of data — and the subsequent addition to piles of open-source intelligence — is becoming a real concern.

I firmly believe we underestimate the significance of the available information — which our enemies recognize — and that a potential adversary can easily acquire.

Let me present a fictitious case study to visualize the problem with the sheer breadth of public data released:

In Europe's High North, where the terrain often is either rocky or marshy, with few available routes for maneuver units, available data will now provide information about ground conditions; type of forest; density; and on-the-ground, verified terrain obstacles — all easily accessible from geodata and forestry agency data. The granularity of the information is down to a few meters.

The data is innocent by itself, intended to limit environmental damage from heavy forestry equipment and avoid the forestry companies' armies of tracked harvesters becoming stuck in the unfavorable ground. The concern is that the forestry data also provides a verified route map for any advancing armored column in pursuit of a deep strike to avoid contact with the defender's limited rapid-response units.

Suppose the advancing adversary paves the way with special forces. In that case, a local government's permitting and planning data and open data for transportation authorities will identify what to blow up, what to defend, and ideal ambush sites for any defending reinforcements or logistics columns. Once the advancing armored column meets up with the special forces, unclassified and openly accessible health department inspections show where frozen food is stored; building permits show which buildings have generators; and environmental protection data points out where civilian fuels, grade, and volume are stored.

Now the advancing column can prepare for the next leg in the deep strike. Open data initiatives, "innocent" data releases, and broad commercialization of public information have nullified the rapid-response force's ability to slow down or defend, and these data releases have increased the speed of the attackers, as well as increased the chance for the adversary's mission success.

And remember this — any US, Canadian, or British units arriving in West European ports face a journey from Rotterdam to the eastern parts of Poland that is the same as that between New York and Chicago. The massive release of open data gives a Russian war planner ample opportunity to fine-tune deep strikes to delay the arrival of these allied forces.

The governmental open-source intelligence problem is a wickedly difficult issue, not least because the solutions are not obvious. Open, democratic states embrace accountability and transparency, and they are the foundations for the legitimacy,

trust, and consent of the governed. Restricting access to machine-readable and digitalized public information contradicts European Union Directive 2003/98/EC, which covers the reuse of public sector information and is a well-established foundational part of European law based on Article 95 in the Maastricht Treaty.

The sheer volume of released information, in multiple languages and from a variety of sources in separate jurisdictions, increases the difficulty of foreseeing its hostile utilization, which increases the complexity of the problem. Those jurisdictions' politics also come into play, which makes it harder to trace a viable route to ensure a balance between a security interest and democratic core values.

But the first steps are clear. Immediate action is required to address this issue, and the West's embedded weakness, and needs to involve both NATO and the European Union, as well as their member states. They should map the crossover points of multinational defense, the national implementation of EU legislation, and the ability to adjust EU legislation for security imperatives.

NATO and the EU have a common interest in mitigating the risks with massive public data releases to an acceptable level that still meets the EU's goal of transparency.

Jan Kallberg, Ph.D., LL.M., is a Non-resident Senior Fellow with the Transatlantic Defense and Security program at the Center for European Policy Analysis (CEPA). He is a former Research Scientist with the Cyber Operations Research Element (CORE) with the Army Cyber Institute at West Point. Dr. Kallberg teaches part-time as a Faculty Member with George Washington University and New York University. He teaches OSINT at the graduate level at NYU. Follow him at cyberdefense.com and @Cyberdefensecom.

Europe's Edge is CEPA's online journal covering critical topics on the foreign policy docket across Europe and North America. All opinions are those of the author and do not necessarily represent the position or views of the institutions they represent or the Center for European Policy Analysis.

James S. Denton Fellowship

Spring 2024 applications are live!

Apply Now

Europe's Edge

CEPA's online journal covering critical topics on the foreign policy docket across Europe and North America.

Read More

Related Articles

Tech’s Regulatory Front Line: App Stores

November 17, 2023

BANDWIDTH DATA AND PRIVACY INTERNET FREEDOM

Cloud Clash: Europe Divides Over Data Digital Sovereignty

November 6, 2023

BANDWIDTH CYBERSECURITY DATA AND PRIVACY

Middle East Violence Tests Europe’s New Digital Content Law

October 13, 2023

BANDWIDTH DATA AND PRIVACY DISINFORMATION

Related Issue Tags

DATA AND PRIVACY EUROPE'S EDGE NATIONAL SECURITY AND INTELLIGENCE

Photo: Seal of the Central Intelligence Agency at its headquarters in Langley, Virginia. Credit: Central Intelligence Agency.