

Eksploitasi sumber data terbuka melalui teknologi informasi pada pengolahan informasi intelijen dalam mendeteksi ancaman (studi kasus pemetaan interaksi antar aktor dalam isu penyadapan Australia terhadap Indonesia) = Exploitation of open sources through information technology in intelligence information processing in the frame work of detecting threats (case study mapping the interaction between actors in the issue of Australian wiretapping against Indonesia) / Radhiatmoko

Radhiatmoko, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20390479&lokasi=lokal>

Abstrak

ABSTRAK

Paska Perang Dingin telah membawa era keterbukaan yang mendorong intelijen untuk lebih beratensi terhadap eksploitasi sumber data terbuka. Meskipun sebelumnya, eksploitasi sumber data terbuka yang dikenal sebagai OSINT sering digunakan dalam proses intelijen, namun nilainya masih dipandang rendah oleh komunitas intelijen. OSINT hanya sebagai bahan sekunder dan pelengkap bagi sumber tertutup. Pandangan tersebut muncul, sebab sumber data terbuka dinilai bukan sumber yang terklasifikasi. Agar menjadi informasi intelijen maka diperlukan validasi dan analisis terlebih dahulu. Pada penelitian ini, teknologi informasi melalui proses text mining digunakan sebagai alat bantu dalam proses eksploitasi sumber data terbuka. Sedangkan pada proses analisisnya menggunakan pendekatan timeline analisis dan social network analisis (SNA). Pendekatan timeline analisis dilakukan untuk menggambarkan interaksi antar aktor terhadap urutan waktu. Sedangkan pendekatan SNA dilakukan untuk memetakan siapa aktor penting pada interaksi antar aktor. Hasil eksploitasi sumber data terbuka yang telah diolah digunakan untuk mendeteksi ancaman atau sebagai early warning dalam mendukung proses analisa intelijen. Deteksi ancaman tersebut dijelaskan dalam tiga sinyal: weak signal (emerging issues), strong signal dan wildcard. Isu penyadapan Australia terhadap Indonesia diangkat sebagai studi kasus dalam penelitian ini untuk menjelaskan bagaimana melakukan eksploitasi sumber data terbuka untuk mendeteksi ancaman.

ABSTRAK

The end of the Cold War has brought about an era of openness that subsequently pushed intelligence to devote more attention to the exploitation of open data sources. Although previously, the exploitation of open source data known as OSINT, is often used in the intelligence process, but the value is still considered inferior by the intelligence community. OSINT is only considered as a secondary and supplementary materials for closed sources. The opinion comes up because open data sources is not considered classified sources. To become intelligence information it needs validation and analysis beforehand. In this study, information technology through text mining process is used as a tool in the process of exploitation of open data sources, while in the process of analysis it uses a analysis timeline approach and social network analysis (SNA). The analysis timeline approach is taken to see the interaction between the actors of the time sequence, while the SNA approach is to map out who is the important actor in the interaction between actors. The exploitation of open data sources that have been processed is used to detect a threat or as an

early warning in supporting the intelligence analysis process. Detection of these threats are described in the three signals: weak signal (emerging issues), strong signals and wildcards. The issue of Australian wiretapping against Indonesia is taken as a case study in this research to explain how to exploit open data sources to detect threats.