

Tackling financial and economic crime through strategic intelligence: The EMPIRES Framework

ANDREWS, Simon <<http://orcid.org/0000-0003-2094-7456>>, POLOVINA, Simon <<http://orcid.org/0000-0003-2961-6207>>, YATES, Simeon and AKHGOR, Babak <<http://orcid.org/0000-0003-3684-6481>>

Available from Sheffield Hallam University Research Archive (SHURA) at:

<http://shura.shu.ac.uk/8635/>

This document is the author deposited version. You are advised to consult the publisher's version if you wish to cite from it.

Published version

ANDREWS, Simon, POLOVINA, Simon, YATES, Simeon and AKHGOR, Babak (2013). Tackling financial and economic crime through strategic intelligence: The EMPIRES Framework. In: ARABNIA, Hamid R., DELIGIANNIDIS, Leonidas, HASHEMI, Ray and LU, Joan, (eds.) Proceedings of The 2013 International Conference on Information and Knowledge Engineering (IKE 2013). CSREA Press, 22-25.

Copyright and re-use policy

See <http://shura.shu.ac.uk/information.html>

Tackling Financial and Economic Crime through Strategic Intelligence: The EMPIRISES Framework

Simon Andrews, Simon Polovina, Simeon Yates, Babak Akhgar
C3RI, Sheffield Hallam University, UK
{S.Andrews, S.Polovina, S.Yates, B.Akhgar}
@shu.ac.uk

Abstract—For the successful monitoring and combatting of Serious Organised Economic Crime (SOEC) and fraud, further integration of Member States systems across Europe is needed. This paper describes a system for strategic intelligence management providing a more coherent and coordinated approach for detecting and deterring SOEC and fraud. The EMPIRISES framework increases the effectiveness of communication between Member States by developing an agreed common language (taxonomy) of SOEC and fraud with automated multi-lingual support. By appropriating and applying existing business tools and analysis techniques to the illegitimate businesses of SOEC and fraud, this new system can support Member States to better target these crimes and the criminals involved.

Index Terms—strategic intelligence management, serious organised economic crime, fraud, business techniques, illegitimate businesses

I. INTRODUCTION

Serious Organised Economic Crime (SOEC) and the associated activity of fraud are growing multinational businesses without respect of national borders. In the European Union (EU) alone these criminal activities cost member states billions of Euros annually. The ability to discover and develop sophisticated new weapons to detect and fight these crimes is thus an imperative. At present, however, each European police force and Financial Intelligence Unit (FIU) has its own Financial SOEC and fraud monitoring system. This severely hampers effective detection and deterrence of these crimes. To be effective at the multinational level requires a collaborative strategy across national systems based on the comprehensive integration of

P. Saskia Bayerl
Rotterdam School of Management, Erasmus University, Burgemeester Oudlaan 50, 3062 PA Rotterdam, the Netherlands, pbayerl@rsm.nl

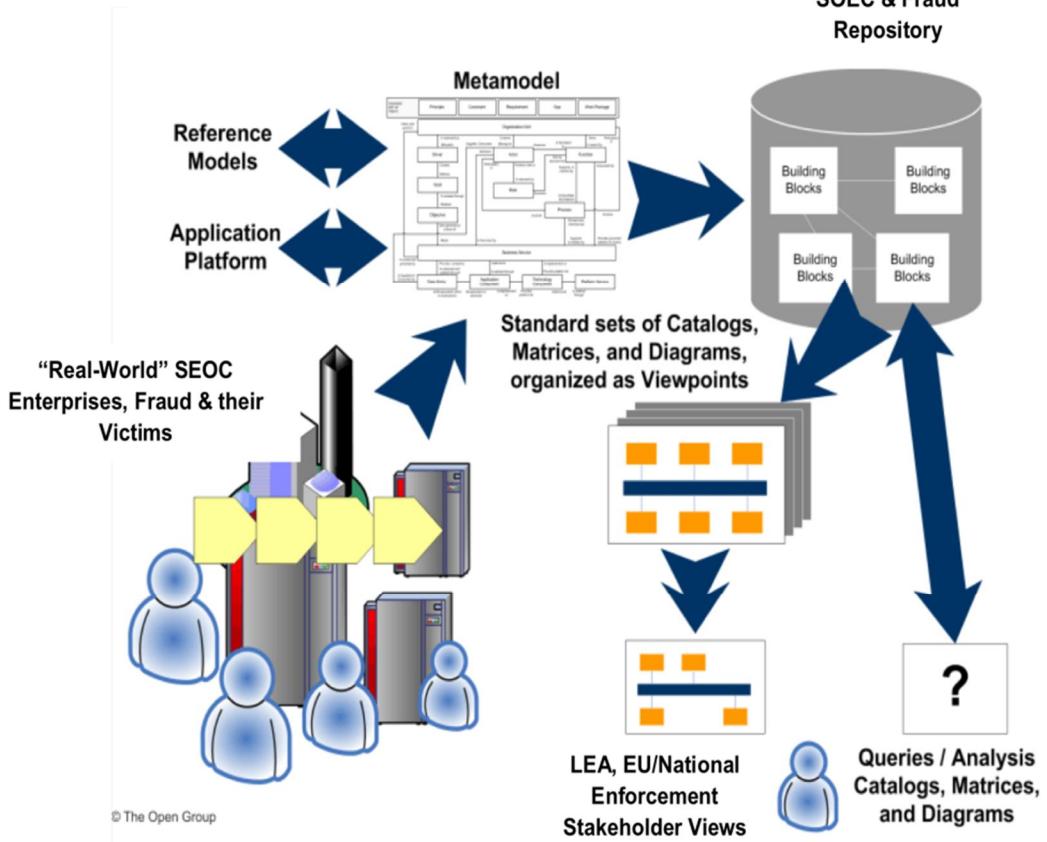
national systems into one multilingual pan-European system. Such a system would federate the large volume of SOEC and fraud information into a single shared inventory of SOEC and fraud. This inventory would employ a pan-European taxonomy of SOEC and fraud capturing even low-level and low intensity activities, hence, providing member states with a comprehensive, common language. It is with this objective in mind that we propose the *Economic criMe PRevention for a Strengthened European Society* (EMPIRISES) framework as a key strategic intelligence asset for law enforcement agencies in combating financial and economic crime.

II. DEVELOPING AN ENTERPRISE ARCHITECTURE OF SOEC AND FRAUD

SOEC and fraud can be described in the framework of Enterprise Architectures (EA). SOEC consists of ‘business’ enterprises just like any other legitimate enterprise, with the difference, however, that the transactions it engages in are inherently unbalanced in their favour. Put simply, SOEC enterprises consider breaking the law as a normal cost of their ‘business operations’. Fraudsters follow the same semantics. Victims to these transactions can be individuals, businesses, organisations or societies as a whole. It is this economic risk and its adverse effects on others that distinguish the structure of SOEC and fraud from other forms of economic activity. Yet, this feature not only serves to differentiate SOEC and fraud from other business activities, it can also be used as a first step to identify and stop their activities.

The EMPIRISES framework employs state of the art knowledge of EA to obtain a clearer understanding of SEOC and fraudulent transactions. With this the EMPIRISES framework provides a solid basis for the application of EA procedures to SOEC and fraud by revealing their fundamental enterprise anatomy. Subsequently, their supply and

Events-Agents (REA) framework [2]. The *Transaction Concept* (TC) identifies the ‘real-world’ agents in enterprise transactions including *how* they transact (the economic events) and *what* they transact (the economic resources) [3, 4, 5]. The TC highlights the value and costs of each transaction as well as its effect on the local, national



consumer chains can be identified and trapped, and/or potential victim(s) alerted. The general framework is based on best practices from the Open Group Enterprise Architecture Framework (TOGAF) [1]. The diagram above is an adaption from TOGAF to illustrate the general structure of SEOC and fraud systems including their protagonists (i.e., the criminal enterprises), their involuntary agents (i.e. the victims) as well as the Local Enforcement Agencies (LEAs) and EU-wide and National Enforcement Bodies aiming to combat these activities..

III. THE SOEC AND FRAUD TRANSACTION CONCEPT IN THE EMPIRISES FRAMEWORK

The conceptualisation of SOEC and fraud transactions in EMPIRISES is based on the Transaction Concept that is based on the Resource-

or international ecosystem. This approach captures the adverse effects on EU economies for each economic resource in a SOEC or fraud transaction, however large or small (e.g., overall social and political impact in the wider ecosystem or loss of state revenues). In the EMPIRISES framework an *economic event* thus details the victim(s) (individual, corporate or jurisdiction) as well as the effects of illegal exchanges of resources for each type of victim. The model differentiates agents according to their location as either inside or outside agents. The *inside agent* is the illicit propagator of the SOEC or fraud, the *outside agent* refers to the victim. Adding these semantics distinguishes the ‘good’ from the ‘bad’ according to the consequences of the transaction.

The Transaction Concept also captures the pragmatics as well as semantics of SOEC, thus

minimising the impact of ‘cat-and-mouse’ games as the SOEC enterprises or fraudsters try to beat the detection system [6, 7]. To capture and represent this complex information, EMPIRES will make use of *Conceptual Graphs* (CGs) [8]. CGs offer conceptual structures. They align the creativity of humans with the productivity of computers, providing knowledge capture and reasoning at this semantic level. Additional rigour is provided at the mathematical level by including a further Conceptual Structure in form of *Formal Concept Analysis* (FCA) [8].

To understand the direct and indirect economic impacts of SOEC and fraud, the Transaction Concept will be combined with *Computable General Equilibrium* (CGE) analysis. CGE is well respected in many fields and used, for instance, in fiscal studies [9, 10, 11]. CGE analysis has demonstrated its capacity to capture the intrinsic mechanisms of the economy to translate inefficiencies through all the productive structures and institutional sectors. Introducing previously identified economic distortions and computing their chained effects in the whole economic system will thus allow a more accurate estimation of the full impact of SEOC and fraud on states [12]. In the context of EMPIRES, a pilot system in form of a *Pan-EU Monitoring System* (PEUMS) will be realised. In a first step, the EMPIRES PEUMS (E-PEUMS) aims at the integration of existing LEA systems in five Member States, namely Finland, Poland, Spain, Turkey, and UK.

IV. THE EMPIRES PAN-EU MONITORING SYSTEM (E-PEUMS)

EMPIRES will be implemented based on the E-PEUMS architecture taking advantage of existing solutions, particularly FIU.NET and SIENA. FIU.NET for Europe together with the Egmont Group works on coordinating and facilitating information exchange between Financial Investigation Units (FIU) on a national and international level. Most EU member states are currently members of FIU.NET. FIU.NET allows members to exchange information on economic crimes using their bespoke MA3tch system. This system allows FIUs to share data in an anonymous way among all members or between specific members by converting data into uniform information. Representatives from member states on FIU.NET range from the Serious Organised Crime Agency (SOCA; a law enforcement but not police agency) in the UK to SEPBLAC in Spain (coordinated by Bank of Spain) to the National Intelligence Unit of the Finnish Police Service.

EUROPOL’s SIENA system provides a similar platform for the exchange of operational information between EUROPOL and its partners in the form of structured data. This system aims to coordinate and assist all member states to maximise collective data sharing and analysis and thus to allow a more detailed and comprehensive picture of available information and intelligence. SIENA uses Analytical Work Files (AWF) to process and analyse data/intelligence it receives from its members. Using this data it supports and helps to coordinate member states on a high strategic level to help tackle serious cross-border criminality.

At present both systems work independently. Still, both organizations acknowledge the need for closer cooperation given the high level of finances associated with serious organised crime.

V. THE ADDED VALUE OF THE EMPIRES SYSTEM

The objective of EMPIRES is to provide an integrative interface to existing databases such as FIU.NET and SIENA. The EMPIRES end-user monitoring systems will allow access, for instance, through the Finish National Police Results Data System (PolStat), the Police Information System (Patja), the West Yorkshire Police intelligence analysis system in the UK, or the Central Intelligence Analysis Unit in Spain.

For this several steps need to be taken to reach beyond existing infrastructures. A known difficulty of traditional RDBMS systems is to represent complex relationships, transactions, actions and events. EMPIRES will employ state-of-the-art RDF triple-store ontology to tackle this issue [14, 15]. This ontology will hold the SOEC and fraud inventory and taxonomy, referred to as the *EMPIRES SOEC and Fraud Knowledge Repository*. Thanks to its knowledge-based architecture, this semantic-web technology is far better suited to express the relational complexity and conceptual, human-based nature of the problem domain [16]. As both RDF and UMF are XML dialects, a simple RDF/UMF conversion will take place as part of data transfer.

EMPIRES will also provide an easy frontend for querying the integrated databases. The RDF query language SPARQL is a powerful tool to exploit the expressivity of ontology, yet normally requires considerable user expertise. EMPIRES will develop simple, intuitive SPARQL Wizards and APIs for all of its SPARQL Endpoint tools to facilitate highly complex queries also for less experienced users. This frontend will build on existing approaches used in FP7 projects such as

CUBIST [16]. For the economic evaluation of SEOC and fraud, EMPRISES will create a set of financial functions (macros) using the recently added SPARQL aggregation functions [15]. EMPRISES will further exploit the popularity and ease of use of existing spread-sheet software, such as Microsoft Excel, by building SPARQL plug-ins for data visualisations such as charts, plots and graphs. By using a simple, ontology-based visualisation of the SOEC and fraud repository, end-users will have a clear view of the underlying data structure and relationships therein. New FCA-based visual analytics will allow extended inventory queries of the underlying SOEC and fraud ontology, allowing semantic, relational, hierarchical, recursive and propagating queries well beyond the current state of the art in traditional data base systems.

VI. CONCLUDING REMARKS

Sharing data and collaborating in the development of pan-European tools and techniques is vital to effectively combat SOEC and fraud. Yet, although basic data exchange is taking place in the EU, there is currently no central repository of SOEC and fraud for EU member states. EMPRISES will support new forms of cooperative analyses by creating a suite of new tools, technologies and techniques to provide new methods of monitoring, detection, evaluation and deterrence of SOEC and fraud. Functionalities include, amongst others, the investigation of effective interventions in SOEC and fraud (e.g., to inform new guidelines and methods of combating and deterring such crimes), the reporting of SEOC and fraud trends, the identification of differences in EU/Country based legislation and tax law, the identification of common modus operandi, situation assessments, economic evaluations of damaged markets, alerts about newly organised investment fraud schemes, predictions of new types of crime by extrapolation of trends and new crime methods, visualizations of the management structure of known groups and gangs as well as early warnings about new SOEC and fraud by matching SOEC's components in several member states. Global and EU businesses, governments and markets can add the EMPRISES architecture to their current sophisticated models, tools and techniques to better detect trends and predict opportunities. This combined approach can thus provide LEAs with better insights and understanding of the crimes and criminal groups that they are investigating and a more powerful way of detecting and deterring such crimes.

REFERENCES

- [1] TOGAF, "Content Metamodel," 2011. [Online]. Available: <http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap34.html>. [Accessed 22 11 2012].
- [2] D. Vymětal and C. V. Scheller, "MAREA: Multi-Agent REA-Based Business Process Simulation Framework," in *ICT for Competitiveness 2012*, Karviná, Czech republic, 2012.
- [3] S. Polovina, "The Transaction Concept in Enterprise Systems," in *Proceedings of the 2nd CUBIST workshop, The 10th International Conference on Formal Concept Analysis (ICFCA 2012)*, Leuven, Belgium, 2012.
- [4] I. Launders, *The Transaction Graph: Requirements Capture in Semantic Enterprise Architectures*, Saarbrücken, Germany: Lambert Academic Publishing, 2012.
- [5] S. Polovina and S. Andrews, "A Transaction-Oriented Architecture for Structuring Unstructured Information in Enterprise Applications," in *Intelligent, Adaptive and Reasoning Technologies: New Developments and Applications*, Hershey, PA, USA, IGI-Global, 2011, pp. 285-299.
- [6] R. Stamper, "Signs, Norms, and Information Systems," in *Signs at Work*, Berlin, Germany, Walter de Gruyter, 1996, pp. 349-397.
- [7] T. Mifflin, C. Boner, G. Godfrey and J. Skokan, "A random graph model for terrorist transactions," in *Aerospace Conference*, 2004.
- [8] S. Polovina, "An Introduction to Conceptual Graphs," in *Conceptual Structures: Knowledge Architectures for Smart Applications*, Berlin - Heidelberg, Springer Lecture Notes in Artificial Intelligence, 2007, pp. 1-15.
- [9] S. Andrews and S. Polovina, "A Mapping from Conceptual Graphs to Formal Concept Analysis," in *Conceptual Structures for Discovering Knowledge (The 19th International Conference on Conceptual Structures, ICCS 2011)*, Derby, UK, 2011.
- [10] S. C. Turner, "Essays on Crime and Tax Evasion, Paper 64," 18 8 2010. [Online]. Available: http://digitalarchive.gsu.edu/econ_diss/64.
- [11] E. B. Sennoga, "Essays on Tax Evasion," Georgia State University, 2006.
- [12] A. Sandmo, "The Theory of Tax Evasion: A Retrospective View," *National Tax Journal*, vol. 58, no. 4, pp. 643-663., 2005.
- [13] R. Meersman, T. Dillon and P. Herrero, On the Move to Meaningful Internet Systems: Confederated International Conferences: CoopIS, IS, DOA and ODBASE, Hersonissos, Crete, Greece, October 25-29, 1010, Proceedings, Berlin - Heidelberg: Springer Lecture Notes in Computer

Science, 2010.

- [14] PR-OWL, “A Bayesian Framework for Probabilistic Ontologies,” 2012. [Online]. Available: <http://www.pr-owl.org/>.
- [15] F. Dau, “Towards Scalingless Generation of Formal Contexts from an Ontology in a Triple Store,” in *Proceedings of the second CUBIST workshop 2012*, Leuven, 2012.
- [16] J. P. Carvalho and J. A. Tomè, “Rule Based Fuzzy Cognitive Maps-Fuzzy Causal Relations,” in *Computational Intelligence for Modelling, Control and Automation*, 1999.
- [17] CUBIST, “CUBIST - Combining and Uniting Business Intelligence with Semantic Technologies,” 14 11 2012. [Online]. Available: <http://www.cubist-project.eu/>. [Accessed 22 11 2012].