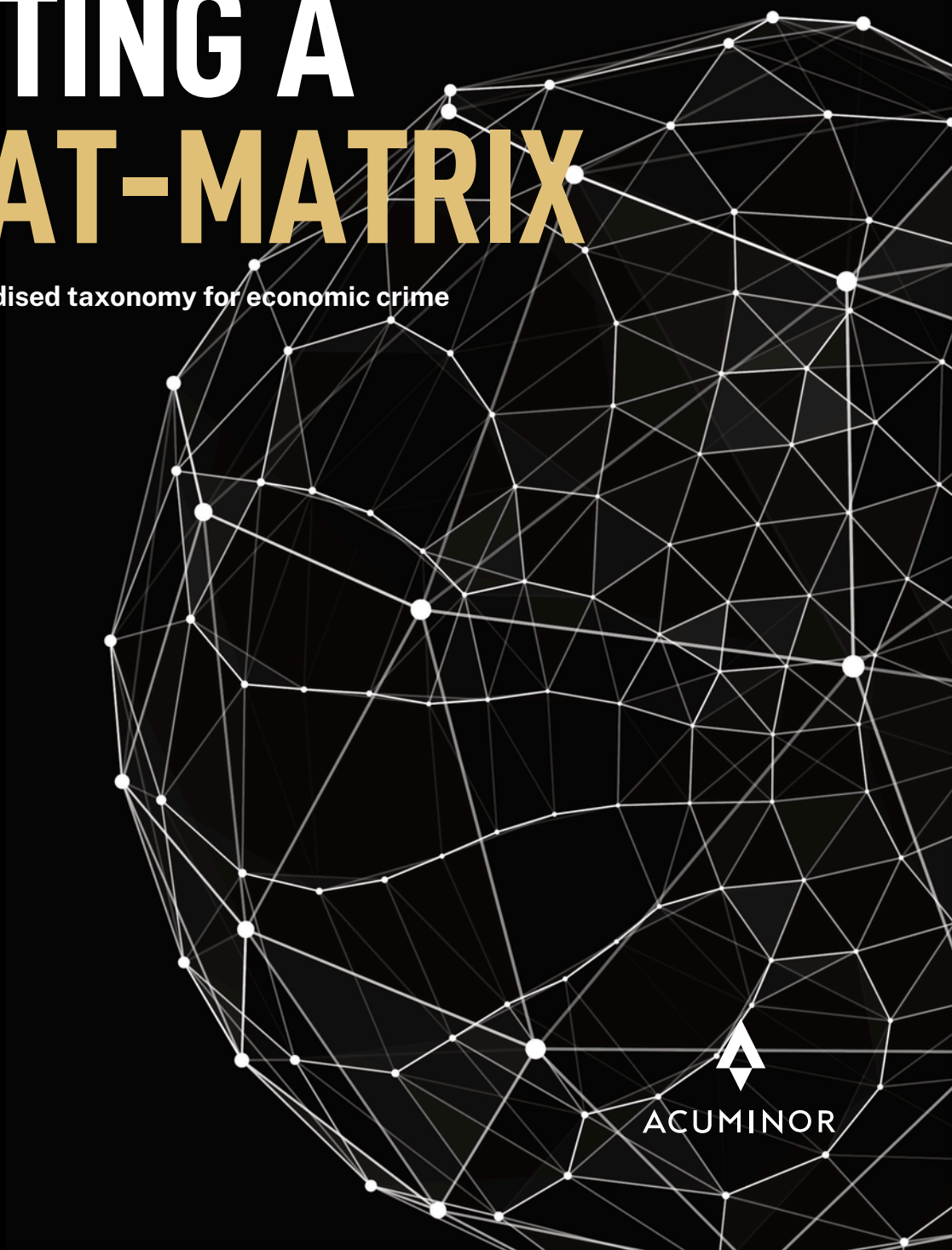
ACUMINOR WHITE PAPER

CREATING A THREAT-MATRIX

The case for a standardised taxonomy for economic crime



ACUMINOR

CREATING A THREAT-MATRIX

Many of you reading this report may have been involved in creating or designing an economic crime 'threat matrix', 'typology library' or similar inside your own organisations. Or perhaps you've been involved in designing a threat-matrix that allows you to communicate with external parties. If so, you will appreciate some of the challenges. If not, you can probably imagine how hard it is to describe and document every economic crime threat your organisation may face in a language that is consistent, actionable and can be understood across the stakeholders involved in detecting and disrupting economic crime.

A threat-matrix should be a dynamic guiding document, one that allows you to understand how criminality perpetrates your organisation and what actions you could take to prevent it.

CHALLENGES FOR THE PRIVATE SECTOR, LAW ENFORCEMENT AGENCIES AND REGULATORS

The challenge to documenting these crimes in a threat-matrix are manifold. Let's take human traffick- ing for instance. Some of the questions you could ask of yourself might include: should you document the typology from the perpetrator's perspective or the victim's? Should you start from the source country or the destination? Is this labour exploitation or sexual or both? Which parts of your organisation are affected and how should that be depicted in the matrix? This is not to mention the challenge of deciding which threats to prioritise with your limited resources.

The potential questions are endless, and the problem only multiples the more crimes you become exposed to. Plus, the threat-landscape is constantly shifting, as new ways to generate and hide illicit money are constantly developed. Even if you do put in the hundreds of man hours needed to create a high-level threat-matrix for one area of your business, **you would have no way of disseminating or industrialising a clear understanding of those threats across the rest of the business units** without an agreed taxonomy that makes sense in the context of the different areas.

Regulators are responsible for setting standards and rules with which firms must comply. The challenge, however, is that regulators often observe the threat landscape from an outside-in perspective. As a result, regulatory reform is often reactive and can lack clear direction as supervisors aren't able to get 'boots on the ground' and understand evolving threat typologies in real-time. Moreover, the combination of cultural change, the introduction of new ways of working and the deployment of novel technologies (e.g., digital assets) significantly increases the workload for regulators in tackling these threats.

Suspicious Activity Reports (SARs) can be difficult for law enforcement to interpret, and the reported risks and typologies often lack sufficient context to connect the crimes to the source. The absence of a common 'language' limits the utility of SARs and significantly slows the response process.

Public-Private partnerships (PPPs) - collaborative arrangements between private institutions and government agencies - provide a pivotal tool in the transition towards an inteligenceled financial crime model. The formation of PPPs is grounded in the premise that there is overlap between the objectives of regulators, law enforcement and the private sector in preventing financial crime. However, information is often shared around a table or via e-mails and is not abstracted to the strategic level so that it can be systematically shared, and the same crime is prevented from happening again across the industry.

A STANDARDISED TAXONOMY FOR ECONOMIC CRIME

A standardised economic crime threat taxonomy provides a solution to many of these challenges. Economic crime is one of the oldest and most established threat landscapes, with fraud and bribery having been around for as long as humans have. Yet, affected parties are comparatively less advanced in their categorisation of such threats, with other industries leading the way.

In a previous report, we highlighted the benefits of similar taxonomies used in the cybersecurity industry, such as the MITRE ATT&CK framework. This globally accessible classification system of cybercrime provides a common, standardised 'language', facilitating the development of more effective threat models and technologies to protect against cyber-related vulnerabilities.

A similar model in the economic crime field would offer guidance as to what kind of threats influence the financial system and assist with refining national and international prevention mechanisms. Such a model would not only outline different threats and techniques, but it would also articulate their potential impacts and provide a historical record of the evolution of economic crime typologies. This, in turn, would enable the private and public sector to pre-empt future developments more effectively and to share information in a more meaningful way. Utilising a technology-enabled economic crime taxonomy would help in the development of common definitions of threats and facilitate more efficient and effective information sharing within PPPs. Such standar- disation would be particularly beneficial in cross-border relationships, since less well understood threats, and their associated impacts, can be easily digested. This would subsequently increase the utility of SARs and enable PPPs to shift the focus from explaining issues to tackling them.

A clear taxonomy and platform to share and add strategic threat intelligence would benefit organisations of all guises by helping to process threat data and to better understand illicit actors, respond faster to incidents, and proactively protect themselves against crime. It would give a basis for the entire eco- nomic crime framework to hang from and would allow a level of communication between the private and public sector which is dynamic enough to keep up with criminal activity.

HOW ACUMINOR'S PLATFORM RISK ASSESSMENT PRO CAN HELP CREATE A STANDARDISED TAXONOMY FOR ECONOMIC CRIME

Acuminor's Risk Assessment Pro (RA Pro) offers a globally accessible, machine-learning powered solution for the analysis of thousands of pages from reliable and vetted sources on economic crime threats and risks.

Users of Risk Assessment Pro can view and analyse a common set of threats and risk indicators to better support disrupting economic crime. Because of the consistent taxonomy and structure, RA Pro provides a basis upon which public or private organisation can add their own internal finding/privileged information on top of Acuminor's database, in a structured that can be used by selected users within the business or a selected group of stakeholders. This allows for intra- or inter-group linkage across threats and risks. **Speaking the same language means that different parties can collaborate on downstream actions taken across the anti-economic crime framework.**

While we acknowledge that technology is only part of the answer to a standardised taxonomy for economic crime, it is an essential piece of the puzzle to systematise and augment existing PPPs. If we are to scale the approach to economic crime with a consistent taxonomy, technology will prove vital.

Acuminor is looking for leaders to join our ongoing ambition to build a systematic approach to sharing strategic financial crime intelligence. Get in touch if you want to be part of developing a highly scalable, standardised approach to financial crime intelligence sharing.

Drottninggatan 71D
111 36 Stockholm
SWEDEN

167-169 Great Portland Street
London W1W 5PF
UNITED KINGDOM

www.acuminor.com
+46 8 121 586 30
sales@acuminor.com