FACEPOINT®
Picture intelligence

THE UNDERESTIMATED THREAT – NARRATIVE SANCTIONS IN THE GLOBAL SANCTIONS REGIME

By Amel Hamza, Subject Matter Expert, FACEPOINT

Over the past weeks, very few words have made it into the news headlines as often as the word sanctions. Trying to stay away from any direct military intervention in the Russia/Ukraine conflict, NATO states and its allies have started an unprecedented sanctions regime against Russian entities and individuals.
For regulated companies and law enforcement agencies, these sanctions come on top of an already incredibly complex global sanctions regime. The idea of simple due diligence by checking an entity or an individual against a self-sustained list has long become unrealistic. Law enforcement agencies face the challenge of limited resources—people and budget—to stay up-to-date with the evolving situation. Providers supporting companies in their AML and KYC obligations are sprouting up everywhere, but few can actually tackle the most challenging piece of all—the narrative sanctions.

Complying with narrative sanctions—reputational risks on top of regulatory risks

Narrative sanctions, or implicit sanctions, refer to organizations or individuals that are not specifically named on a certain list, but that are still considered as sanctioned. This creates a challenge for organizations, as there is no finite sanction list to follow. Complying with the so called 50% rule is something which is a pain for regulated organizations. For example, if a listed individual has 50% or more ownership of a non-listed entity, EU citizens or entities are prohibited from making funds and economic resources available to that entity. It is worth remembering though, that organizations are set up and registered somewhere. A paper trail exists. Names can be found. With enhanced due diligence it is mostly possible to find out the ultimate owner and comply with the sanctions.
This could cover the regulatory risks an organization is facing in today's sanctions regime, but what about the reputational risks? What if you find yourself in the situation that you just opened a bank account for a fighter working for a paramilitary organization? Or if you opened your borders to individuals of other politically violent groups or terrorist organizations?

Narrative sanctions in the context of terrorism and political violence

While enhanced due diligence can get you relevant results at some point, the topic of narrative sanctions becomes more complicated when we look beyond listed organizations. In many cases, sanctions are introduced to target organizations that are classified as criminal groups by the entity imposing them, such as the UN or the EU. However, criminal organizations do not have an employee directory. They are often loosely knit groups fighting for a common cause under a structure that is extremely difficult to penetrate. Even enhanced due diligence would often not be successful, given that there is no name of a person of interest or any other data available to base the search on.
In such cases, biometrical search is the only option to manage the high regulatory and reputational risks. With a database of images, companies and law enforcement agencies can identify members of criminal groups that are not namely known by the regulator simply by matching a face against the database.

FACEPOINT®
Picture intelligence

THE UNDERESTIMATED THREAT – NARRATIVE SANCTIONS IN THE GLOBAL SANCTIONS REGIME

By Amel Hamza, Subject Matter Expert, FACEPOINT

Criminal organizations and sanctioned violent political groups produce content (videos or pictures) to promote their ideology. This footage can be analyzed by subject matter experts. For each individual identified, a profile is set up in the database that is then continuously enhanced with more details. As soon as the picture profile is created, organizations using the database can identify a certain individual as a person of interest—and act accordingly.

This unique identification mode is particularly relevant for the identification of dangerous actors. For example, individuals trying to hide their involvement in fighting under the Islamic State banner could be identified in a video and inserted into the database for participation in a terrorist/criminal organization.
For notoriously closed entities, for example the Regime of the Democratic People's Republic of Korea, a deep investigation of their communication networks and contents can lead to the identification of persons of interest that are not identifiable through a traditional WEBINT search. Indeed, it is particularly difficult to find information on high-value individuals who know how not to be detected. Both criminals and terrorists use aliases to escape identification. However, biometrical data cannot be faked.
The current situation in Ukraine is a good illustration of the coverage and staging of sanctioned armed groups that are taking part in the conflict. These contents have much more to say about persons of interest than sanctions lists.

A holistic approach to sanctions

The headache to comply with a complex sanctions regime for regulatory, but sometimes also moral, reasons is not new. Organizations have either large legal departments to work on the issue or reach out to providers to support them. Law enforcement agencies are trying their best to keep their own databases up-to-date. However, limited time and budget is the common nominator of the public and private sector. The high reputational risks are asking for a new approach to sanctions beyond the tick-the-box exercise of traditional methods and even enhanced due diligence. With a database based on face biometrics, no person of interest will be able to hide behind aliases or fake ID credentials anymore.

About FACEPOINT
FACEPOINT's database is an exclusive photographic database of over 1.4 million profiles and over 3 million pictures. Profiles are generated through open source intelligence and user-generated content, made available to the public. In order to enable compliance and risk professionals to clarify or confirm any possible overlap between their records and those in FACEPOINT's database, FACEPOINT's research team strives to find as many identifiers of individuals or entities as possible from publicly available information. Sanctions lists are monitored by a dedicated sanctions team. For each individual listed, the team, composed of OSINT specialists, makes a special effort to find the associated faces. The main sanctions lists are monitored daily and immediately updated by an analyst.