Analistler için

Siber Suç İstihbaratı

El Kitabı

İçindekiler

1. İstihbarata giriş

BİLGİDEN İSTİHBARAT

Bilgileri, istihbaratı ve analizi teorik ve pratik terimlerle doğru bir şekilde tartışıp keşfetmeden önce, bu terimlerin ne anlama geldiği konusunda ortak bir anlayışa sahip olmamız gerekir. Bu üç anahtar terimin bazı tanımları aşağıdaki gibidir:

Bilgi

- Ham formda bilgi

İstihbarat

- Anlaşılabilir bilgi
- Katma değerli bilgiler
- Kaynağı ve güvenilirliği bağlamında değerlendirilen bilgiler

Analiz (bilgi veya istihbarat)

- Bir şeyin çözümlenmesi veya bileşenlerine ayrılması
- Bu parçaların tespiti
- Arkalarındaki genel ilkeleri keşfetmek için şeylerin kaynağına kadar izlenmesi
- Bu sürecin sonuçlarının bir tablosu veya ifadesi

Bu terimler arasındaki farkı ve nasıl etkileşime girdiklerini doğru bir şekilde anlamak önemlidir, ancak bu erken aşamada bile bu tanımlar temel farklılıklara işaret etmektedir. Bilgi, herhangi bir türden oldukça basit bir şekilde ham veridir, buna karşın istihbarat, üzerinde çalışılmış, katma değer veya önem verilmiş verilerdir.

BİLGİ + DEĞERLENDİRME = ISTIHBARAT

Bu dönüşümün yapılma yolu, bilgiyi kaynağı ve güvenilirliği ile bağlamına göre değerlendirme süreci olan değerlendirmeden geçer.

En basit haliyle, istihbarat analizi, bilgiyi toplamak ve kullanmak, onu istihbarata dönüştürmek için değerlendirmek ve daha sonra bilinçli karar vermeyi desteklemek için ürünler üretmek için bu istihbaratı analiz etmekle ilgilidir.

1

Tüm bu kararlar, bilgiyi "analiz etme" konusundaki doğal yeteneğimizi, faydalı bir şekilde bir dizi aşamaya bölünebilen genel bir süreci veya kendimize şu şekilde sorduğumuz soruları içerir:

" Sorun tam olarak nedir; hangi kararı vermemiz gerekiyor ve neden önemli veya önemli?
" Elimizde mevcut sorunla ilgili olabilecek hangi bilgilere sahibiz veya makul bir şekilde elde edebiliriz. Nerede/nasıl alabiliriz?
" Bilgiden hangi anlamı çıkarabiliriz; neler olduğu hakkında bize ne anlatıyor?

" Tek bir olası açıklama var mı, yoksa başka alternatifler veya seçenekler var mı? Bazıları diğerlerinden daha olası mı?
" Bunlar, vermemiz gereken kararı nasıl etkiler, bazı seçenekler potansiyel olarak diğerlerinden daha iyidir; bazıları daha büyük başarı ve/veya başarısızlık riski taşıyor mu?
" Makul bir güvenle harekete geçmeye hazır mıyız yoksa önce daha fazla bilgi mi toplamamız gerekiyor? Eğer öyleyse, başka neye ihtiyacımız var ve nereden/nasıl alabiliriz?

Bu soruları uygulama, cevapları değerlendirme ve ardından nasıl yanıt verileceğini ve harekete geçileceğini seçme süreci, analizin neyle ilgili olduğunun özüdür.

Bu süreci bilinçli kontrolümüz altına alarak izleyebilir, geliştirebilir, iyileştirebilir ve kavraması oldukça karmaşık olabilecek kalite kontrollerine tabi tutabiliriz. Bu farkındalık ve beceri gelişimini başlatmak çok önemlidir. Bireyin analitik becerilerini geliştirmenin pratik avantajları çoktur, ancak şu şekilde özetlenebilir:

ANALİZ GERÇEKLERİN ÖTESİNE GİDER
Size bilginizin/istihbaratınızın ne kadar iyi (veya zayıf) olduğunu söyleyebilir.
Size daha önce bilmediğiniz şeyleri söyleyebilir
Bir durumu anlamak için bilmeniz gerekenleri size söyleyebilir.
Size daha fazla nereye bakmanız gerektiğini söyleyebilir
Anladığınızı başkalarına iletmenize yardımcı olabilir

İstihbarat analizinin kökenleri

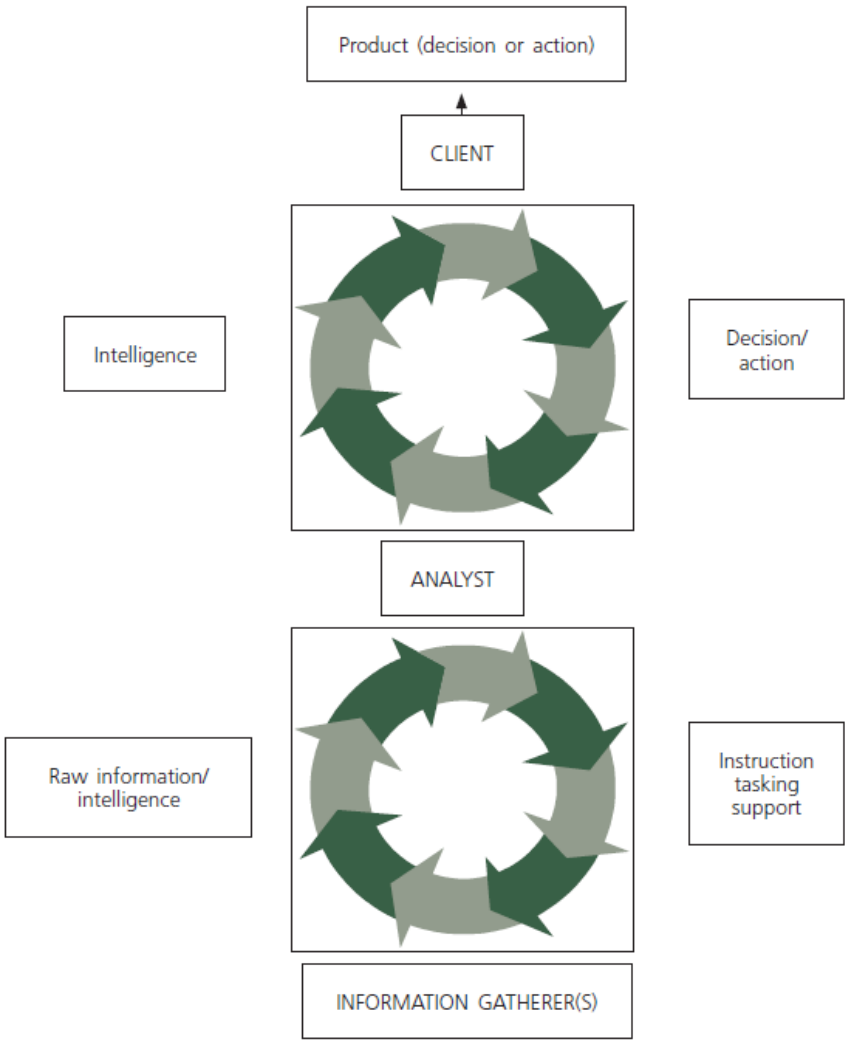
Bilgi, güce eşit olma potansiyeline sahiptir. Resmi, yapılandırılmış bir şekilde karar vermeyi desteklemek için bilgi toplama ve kullanma kavramı yeni bir şey değil. Rakiplere karşı avantaj elde etmek için, diğer şeylerin yanı sıra, niyetleri ve yetenekleri hakkında en güncel, doğru bilgilere sahip olmak zorunludur. Bu kural, politika, iş, askeri strateji veya suç istihbaratı olsun, her alanda geçerlidir. Ayrıca, sosyal/kültürel faktörlerdeki, teknolojideki, *organizasyonel* ihtiyaçlardaki ve yeni/daha yüksek analitik beceri seviyelerindeki değişikliklere yanıt olarak her zaman sürekli gelişen ve gelişen bir süreçtir .

Bir süreç ve bir meslek olarak istihbarat ve analizin tarihsel arka planını, "köklerini" gözden geçirmek faydalı ve önemli bir alıştırmadır. Istihbaratın ve analizin kökenlerine ilişkin anlayışımızı geliştirmek, hem şu anda nerede olduğumuzu hem de bu noktaya nasıl/neden geldiğimizi anlamamıza yardımcı olur. Aynı zamanda, istihbarat analizinin nasıl sürekli değişen, gelişen bir uygulama olduğu ve pratik anlamda alakalı ve yararlı

kalması için sürekli olarak taze, esnek bir yaklaşıma, yeni fikirlere, yeni becerilere, yeni tekniklere ihtiyaç duyduğu konusunda farkındalığımızı arttırır. Profesyonel istihbarat analisti için değişmeyen tek şey, iki görevin veya projenin asla tamamen aynı olmamasıdır; her yeni iş parçası yeni bir yaklaşım gerektirir.

Tarih boyunca askeri, dini ve cemaat liderlerinin aktif olarak bireyleri bilgi toplama tatbikatlarıyla görevlendirdiği ve daha sonra kararlarını bu şekilde elde edilen bilgilere dayandırdığı birçok örnek vardır. Bilgi toplama ve istihbarata dayalı eylemler konusunda belki de bilinen en eski metin, Çinli bir paralı asker olan Sun Tzu tarafından MÖ 5. yüzyılda yazılan "Savaş Sanatı, Strateji Sanatı"dır. Başarısı, etkili bilgi toplama ve istihbarata dayalı karar alma yeteneğine çok şey borçlu olan askeri seferlere komuta etme yeteneğiyle ünlüydü. Bugün hâlâ basımı devam eden bu çalışmanın kalitesi hakkında çok şey söylüyor ve dünya çapındaki askeri ve kurumsal stratejistler ve istihbarat ajanları için temel bir okuma. Tarih boyunca bu erken başlangıçlardan görece yakın zamanlara kadar, bilgi toplayıcıların öncelikle askeri amaçlar için kullanılması yaygın bir eğilim olmuştur.

Dahası, bu süreçten temel olarak bilgi toplayıcı(lar) ile müşteri/karar verici arasında doğrudan teması içeren, şekil 1-1'de gösterildiği gibi bir metodoloji ortaya çıkmıştır:



Şekil 1-1. Temel görev modeli

Bu yöntemin bazı dikkate değer özellikleri vardı:

1) Dahil edilen saf lojistik (ulaşım veya iletişim için gerçek bir teknoloji yok), bilgi toplayıcının görevlendirilmesi, bilginin elde edilmesi ve bilginin "son kullanıcıya" teslim edilmesi arasında büyük bir zaman gecikmesi yarattı.

2) Mekanları ziyaret ederek ve olaylara bizzat veya aracılar aracılığıyla tanık olarak faaliyet gösteren bilgi toplayıcıları kullanmak, toplanan bilgilerin duyuları ve gördüklerini doğru bir şekilde hatırlama yetenekleri ile sınırlı olacağını garanti etti; bu tür bilgiler bu nedenle her zaman oldukça öznel olacaktır ve gerçeklerden ziyade görüşlere dayanma eğiliminde olacaktır.

3) Bu kadar büyük bir zaman ve kaynak yatırımı karşılığında toplanan bilgi hacmi son derece küçük olacaktır.

Herhangi bir araştırma, büyük miktarda bilgi üretir; soruşturma ne kadar büyük olursa, araştırmacının uğraşması gereken o kadar fazla bilgi olur. Müfettişler için sorun şu ki, sistem tüm bu bilgileri ne kadar iyi depolarsa saklasın, her zaman bilgiyi bir bütün olarak kucaklamak, bir kerede "hepsini almak" için kendi zihinsel kapasiteleriyle sınırlıdır.

Bilginin tamamının bu şekilde anlaşılması, geçerli karar verme için çok önemlidir. Mevcut tüm bilgilerin küçük bir bölümünü tam olarak anlamak, aslında araştırmacının tüm durumu yalnızca kısmen anladığı anlamına gelir.

KISMİ ANLAYIŞ BİR DERECE YANLIŞ ANLAŞMA İÇERMELİDİR.
YANLIŞ ANLAYIŞ, KÖTÜ SONUÇLARA YOL AÇAR.

Bu potansiyel olarak sakatlayıcı sınırlamalara rağmen, sürecin bu zamanlar boyunca askeri ve siyasi kampanyaların başarısında hala belirleyici bir faktör olduğunu kanıtlaması, istihbarat ve analizin öneminin ve değerinin bir ölçüsü olarak makul olarak alınabilir.

Bilgi edinme yöntemleri, geçen yüzyılın sonlarına doğru tarih boyunca çok yavaş değişti. O zaman başlayan ve bugün hala devam eden teknolojideki muazzam büyüme, bilgi toplama yöntemlerinde büyük bir değişiklik olduğu kanıtlanan şeyi getirdi ve bu da analiz ve istihbarat için yeni yaklaşımlar için bir talep yarattı.

Bu süreç, 19. yüzyılın sonlarında, mesajların giderek daha büyük mesafelere neredeyse anında gönderilmesine izin veren telgraf ve telefonun ortaya çıkmasıyla başladı. Bu, bir anda, bilgi toplayıcının kaynak ve istemci arasında hareket etmesine duyulan ihtiyaç nedeniyle eski yöntemlerin maruz kaldığı kaynak ve zaman sorununu ortadan kaldırdı. Bu değişiklik beraberinde bir takım faydaları da getirdi.

İlk olarak, bir müşterinin bilgi istemesi ile sonucu alması arasındaki "yanıt süresi" büyük ölçüde azaltıldı; bu, müşterilerin bu tür bilgilere dayanarak hızlı tepki verme yeteneğini

geliştirdiği için açık bir faydayı temsil ediyordu. Buna ek olarak, bu gelişme aynı zamanda bilgi kaynağının aktarım sırasında bilgiyi "unutması" veya "kaybetmesi" için daha az zaman olması ve dolayısıyla bilgi kalitesinin artması nedeniyle zincirleme bir fayda sağlamıştır. Benzer şekilde, bilginin fiziksel olarak müşteriye geri taşınmasına ihtiyaç duyulmaması, kaynaklarda büyük bir tasarruf sağladı; bilgi toplayıcılar seyahat etmeye/bilgi aktarmaya daha az zaman ayırabildiler ve dolayısıyla bilgi toplamaya daha fazla zaman ayırabildiler.

Bu değişikliğin genel sonucu, ironik bir şekilde, bu faydaların müşteri için yeni bir sorunu da beraberinde getirmesiydi. Eskisinden çok daha hızlı bir şekilde çok daha büyük miktarlarda bilgi toplandı ve karar verme tepki süresi azaldı. Ek olarak, bilgi toplama sürecinin kendisinin kontrol edilmesi, yeni, geliştirilmiş performanslarının bir sonucu olarak oluşturulan bilgi toplayıcılar için yeni görev ve düzenlere daha fazla vurgu yapılması için yeni bir ihtiyaçla birlikte bir sorun haline geldi.

Bu nedenle, yeni sistem bir bilgi "aşırı yüklenmesi" yarattığı için, sürecin bilgi toplayıcı ve müşteri arasında bilgi geçişini içerdiğinden önce, müşterinin alınan tüm bilgileri etkili ve hızlı bir şekilde işleyemediği ve daha sonra buna tepki veremediği yeni bir sorun ortaya çıktı. .

analist

Müşterinin, bilginin hızlı yorumlanmasını ve karar vermesini sağlayan bir duruma geri dönmesi gerekliliği ortaya çıktı. Bu, bilgi toplayıcı ile müşteri arasında, bu sürecin sonucu müşteriye iletilmeden önce, bilginin büyük kısmının alınabileceği, kaydedilebileceği, değerlendirilebileceği ve yorumlanıp anlam çıkarmak için incelenebileceği bir ara aşamaya ihtiyaç yarattı. Bu, bir analistin işlevinin kökeniydi ve süreç, şekil 1-2'de gösterildiği gibi bugün de özünde aynı kalıyor:[1]

Analistin temel işlevi aşağıdaki gibi üç aşamalı bir sürece ayrılabilir:

" Bilgi toplamak, onu anlamak ve her bir parçanın diğerleriyle olan ilişkisini veya ilişkisini anlamak.

" Bütün hakkında bir anlayışa varmak için bu bilgiyi nesnel olarak geliştirmek.

" Bu anlayışı başkalarına iletmek ve böylece istihbarat sürecini pratik kullanıma sokmak.

Problemler

Bu yeni metodoloji geliştikçe ve bilgi kaynaklarının çeşitliliği, kapsamı ve erişilebilirliği genişledikçe, sonuç, göreceli olarak konuşursak, "analist" işlevinin boyut, sayı ve etki açısından büyümesiydi. Basitçe söylemek gerekirse, daha fazla bilgi "merkeze" geri

[1]Analiste ham bilgi veya istihbarat şeklinde değerlendirilmiş bilgi veya her ikisi birden sağlanabilir.

aktarıldıkça ve istihbarata dayalı karar alma sürecine daha fazla güvenildikçe, kuruluşlar istihbarat üretmek, yaymak ve analiz etmek için giderek daha fazla insanın bilgiyi değerlendirmesi gerektiğini keşfetti.

Devam eden bu durumun, günümüzün istihbarat birimleri ve analitik personeli üzerinde etkileri vardır. Toplanan daha fazla bilgi, analize ve dolayısıyla karar vermeye daha fazla yardımcı olur. Bununla birlikte, daha sonraki iş yükünü de arttırır, bu da personelde ve üretkenlikte bir artışa veya etkinlik kaybına neden olur. Basit bir ifadeyle, analitik ürüne olan artan ihtiyaçla birlikte analiz edilecek bilgideki artış, daha fazla/daha iyi eğitimli analistlerin sunabileceği gelişmiş verimliliği her zaman aşma eğilimindedir. Başka bir deyişle, etkili, profesyonel analitik süreç, kendi üzerine daha fazla çalışma getirme eğilimindedir.

Suç istihbaratı analizi

"Suç istihbaratı" nedir? Suç müfettişleri de dahil olmak üzere çoğu insan için bu terim, suç ve suçlular hakkında topladığımız bilgileri depolamak ve almak için kullanılan harmanlayıcı tarzı sistemlerin görüntülerini çağrıştırır. Topladığımız bilgilerin hacmi ve çeşitliliği genişledikçe, depolanmasına ve alınmasına yardımcı olmak için giderek daha karmaşık sistemler tanıttık. Bu sınırlı bağlamda bakıldığında, bilgi teknolojisinin (BT) tanıtılması kayda değer bir başarı olmuştur; Suç bilgilerinin saklanması ve geri alınması için BT'nin kullanılması, artık operasyonel ceza soruşturmacısı için neredeyse ikinci bir niteliktir ve bu araçlar olmadan, bir hizmet olarak, kayıt ve suç bilgilerinin harmanlanması.

Bilgi toplamak başlı başına istihbarat elde etmekle sonuçlanmaz. Bilgi, üzerinde işlem yapılmadan önce uygun şekilde değerlendirilmelidir. Suç istihbaratının değeri analizle daha da artırılabilir. Mevcut istihbarat, basit eylem için çok karmaşık ve hacim olarak büyük olduğunda, anlamlı sonuçların elde edilebilmesi için analiz edilmesi gerekir.

Halihazırda, suç veya suçlular hakkında topladığımız bilgilerden, gerçek "suç istihbaratı" geliştirmek için, gerek istihbarat birimlerinin kendileri gerekse müşterileri, operasyonel suç araştırmacıları tarafından yetersiz şekilde kullanılabiliyor. Suç istihbaratına kolay erişim ve depolama için tüm yeni sistemlerde bile, araştırmacılar bu bilgiyi doğru bir şekilde değerlendirmedikçe ve analiz etmek için analistleri kullanmadıkça, bu paha biçilmez kaynağı gerçeklere "hazır referans" olarak kullanmaktan başka bir şekilde gerçek anlamda kullanamayabilirler. Bu sürecin ürettiği istihbarat.

Kriminal istihbarat analizi (CIA), suç ve suçlular hakkında topladığımız istihbarat ve bilgileri kullanarak soruşturmaya nasıl yaklaşabileceğimizi ortaya koyan bir felsefedir. Doğal tümdengelim güçlerimizi ve düşünce süreçlerimizi yapılandıran teknikleri, yetkin araştırmacıların her zaman bilinçaltında kullandığı "doğal sezgiyi" sağlar. Ayrıca, topladığımız bilgileri anlamamıza ve bu anlayışı başkalarına iletmemize yardımcı olan araçlar sağlar.

ileriye giden yol

Suç istihbarat analisti, operasyonel araştırmacı kadar bir suç araştırmacısıdır. CIA'nın operasyonel bir araç olarak değerli olmasının anahtarı, analiz sonuçlarının soruşturma için doğrudan değerde olması gerektiğidir. O zaman en iyi sonuçların ancak analist ve araştırmacı aynı ekibin ayrılmaz parçaları olan ortaklık içinde birlikte çalıştığında elde edilebilir.

Aynı şekilde, analist ve dedektif de iyi bir suç araştırmacısı olmak için gereken aynı becerilerin çoğunu paylaşmalıdır. İstihbarat analistleri için temel sorun, istihbaratı ve bilgiyi organize bir şekilde bir araya getirmektir, böylece bir araya getirilen bilgiden anlam çıkarmak gibi zor bir görev daha kolay hale gelir. Yalnızca orijinal bilginin ne anlama geldiğine dair uygun açıklama türetildiğinde, bu istihbarat pratik kullanıma sokulabilir. Bu kılavuzda yer alan teknikler ve sistemler, herhangi bir araştırmada değerli olabilecek pratik araçlardır.

İstihbarat analizi ve organize suç

Suç istihbaratı analizinin ortaya çıkışı, bireysel suçun organize veya grup suçuna dönüşmesiyle doğrudan bağlantılıdır. İstihbaratın etkin kullanımı, bir kolluk kuvvetinin suç gruplarıyla mücadele yeteneği için çok önemlidir. İstihbarat analizi ayrıca ajansa kaynaklarının etkin yönetimi için gerekli bilgiyi sağlar. Uygun görevlendirme ile istihbarat analizi ürünleri, mevcut sorunların üstesinden gelmek ve gelecekte beklenen sorunlara hazırlanmak için stratejik planların geliştirilmesine yardımcı olabilir.

Suç istihbarat analizi, kolluk kuvvetlerinin suça karşı proaktif bir yanıt oluşturmasına izin verir. Kendi alanlarında faaliyet gösteren suç gruplarını belirlemelerini ve anlamalarını sağlar. Suç grupları belirlendikten ve alışkanlıkları bilindikten sonra, kolluk kuvvetleri, tahmin etmek ve gelecekteki suç faaliyetlerinin gelişimini engellemek için suçtaki mevcut eğilimleri değerlendirmeye başlayabilir. İstihbarat, kararların dayandırılacağı ve araştırma için uygun hedeflerin seçileceği bilgiyi sağlar. Suç istihbaratı analizinin kullanılması, soruşturmaları, gözetim operasyonlarını ve davaların kovuşturulmasını desteklemek için uygun olmakla birlikte, kolluk kuvvetlerine kaynakları, bütçeyi etkin bir şekilde yönetme ve suç önleme sorumluluklarını yerine getirme becerisi de sağlar.

Geçen yüzyılın şafağında, "organize suç" Cosa Nostra ile eş anlamlıydı. Bugünkü organize suç tablosu oldukça farklı. İyi gelişmiş örgütsel yapılara sahip yeni suç gruplarının çoğu, güç ve zenginlik elde etmek için kurulmuştur. Bu gruplar arasında kanun kaçağı motosiklet çeteleri, Rus organize suçları, Asya organize suçları, Afrika organize suçları, uyuşturucu kartelleri ve sayısız sokak çetesi -Asyalı, Koreli, Hispanik, siyah, beyaz üstünlüğü, bunlardan sadece birkaçı sayılabilir. Batı Afrika suç şebekeleri gibi neredeyse yapısız akışkan ağların gelişmesiyle karmaşıklık seviyeleri daha da artıyor. Farklı organize suç grupları ve ağları arasındaki işbirliğinin yaygın olduğu unutulmamalıdır.

Suç grupları insan ticareti, uyuşturucu kaçakçılığı, gasp, dolandırıcılık ve cinayet gibi girişimlerde bulunmaya devam ediyor. Bazıları şimdi yüksek teknoloji suçları gibi yeni suç girişimlerine giriyor. Son birkaç yılda İnternet kaynaklarının patlaması, suçlular için yeni mali kazanç fırsatları yarattı. Yüksek teknoloji suçlarındaki bu artış, kolluk kuvvetleri için zorlu ve nispeten yeni bir alandır.

Suç örgütleri her zamankinden daha sofistike ve dinamik. Kolluk kuvvetlerinin önündeki zorluk, suç faaliyetlerinin topluluklarımız üzerindeki etkisini azaltmak için bu artan karmaşıklığa hazırlıklı olmaktır.

Bunu başarmak için kolluk kuvvetlerinin, organize suç grupları tehdidine karşı koymak için ileriye dönük, iddialı ve kapsamlı stratejilere ihtiyacı vardır. Suç istihbaratı analizi, görevlendirildiği ve etkin bir şekilde kullanıldığında, kolluk kuvvetlerinin cephaneliğinde önemli bir varlık olabilir. Birleşik Krallık gibi kriminal istihbarat konusunda daha fazla deneyime sahip ülkeler, kriminal istihbaratın nasıl kullanıldığını standartlaştırmaya yardımcı olmak için ulusal istihbarat modelleri geliştirmiştir.

Bilgi teknolojisi, istihbarat paylaşımının anahtarıdır. Özellikle terörizm de dahil olmak üzere karmaşık çok uluslu suç çağında, istihbarat ve bilginin etkin bir şekilde paylaşılmaması, tüm devletlerin terörle mücadele çabalarını sınırlandırmaktadır.

2. İstihbarat süreci

İSTİHBARAT

Istihbarat kelimesi, bilgiyi anlamlandırmak için yorumlama sürecini tanımlamak için kullanılabilir. Aynı zamanda, bu tür bilgileri toplayan veya bunlarla ilgilenen bir grup veya departmanı tanımlamak veya bu tür faaliyet veya departmanın ürününü tanımlamak için de kullanılmıştır. En basit haliyle istihbarat, işlenmiş bilgi olarak tanımlanabilir. Kolluk kuvvetlerinin kullanımına indirgenen "istihbarat", adli soruşturmalara karar vermek ve desteklemek için kolluk kuvvetlerinin faaliyetleri tarafından elde edilen, istismar edilen ve korunan bilgiler olarak tanımlanabilir.

ISTIHBARAT: EYLEM İÇİN TASARLANMIŞ BİLGİ (İŞLENMİŞ BİLGİ)

İstihbarat her zaman kaçınılmaz derecede spekülasyon ve riskle sonuçlanan bir dereceye kadar yorumlama içerir. Spekülasyon ve risk miktarı, bilginin kalitesine ve miktarına bağlıdır. İstihbarat genellikle iki ana alana ayrılır:

Stratejik istihbarat : Kolluk kuvvetlerinin uzun vadeli amaçlarına odaklanır. Tipik olarak, suç ortamındaki mevcut ve ortaya çıkan eğilimleri, kamu güvenliği ve düzenine yönelik tehditleri, eylemleri kontrol etme fırsatlarını ve karşı programların geliştirilmesini ve politika, program ve mevzuatta değişiklik için olası yolları gözden geçirir.

Operasyonel istihbarat : Tipik olarak, bir soruşturma ekibine herhangi bir tür yasadışı operasyonun belirli unsurlarına ilişkin hipotezler ve çıkarımlar sağlar. Bunlar, kanuna aykırı faaliyetlerde bulunan belirli suç şebekeleri, bireyler veya gruplar hakkında hipotezleri ve çıkarımları içerecek ve etkili kanun uygulama eylemi için kullanılabilecek yöntemlerini, yeteneklerini, güvenlik açıklarını, sınırlamalarını ve niyetlerini tartışacaktır.

İyi bir operasyonel istihbarat bilgisi, stratejik istihbarat yeteneği geliştirmek için şiddetle tavsiye edilen bir ön koşuldur. Operasyonel istihbaratın kendi içinde geliştirilmesi, stratejik bir perspektiften ele alınması gereken önemli bir istihbarat kaynağı sağlayacaktır.

İSTİHBARA KARŞI KANIT

Bir devletin ulusal mevzuatının, istihbaratın kolluk kuvvetleri için nasıl kullanılacağını belirleyeceğini vurgulamak önemlidir. Belirli bir soruşturmayla ilgili istihbarat toplama süreci, genellikle herhangi bir

kanıt toplama aşamasının başlangıcıdır. Mevzuat ayrıca, bir soruşturma sırasında toplanan istihbarat materyalinin cezai takibatta ifşa edilmekten korunup korunmadığını da belirleyecektir.

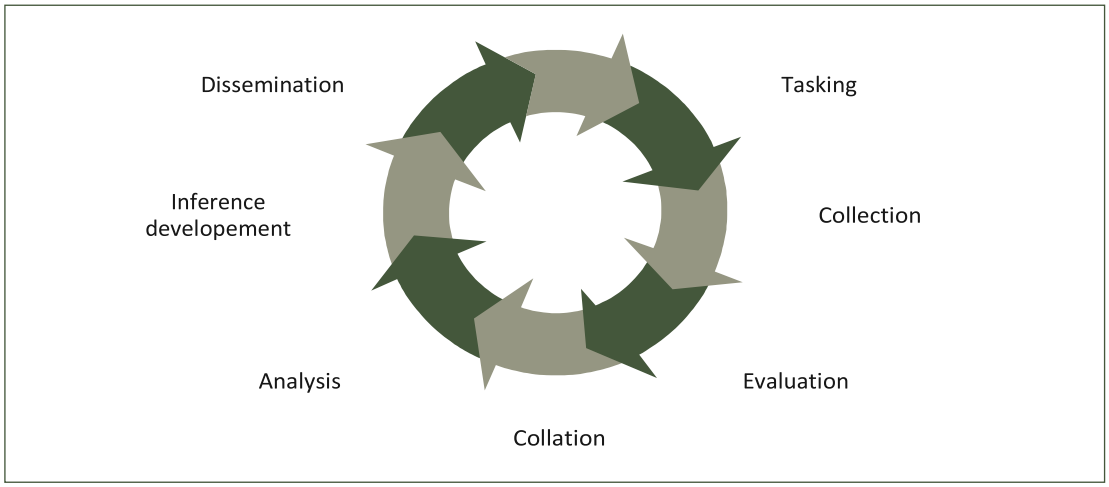
DELİL: KANIT OLUŞTURULACAK VERİLER

Soruşturmanın bu kısmı, bildirilen olaylara yanıt verir ve ne olduğunu ve kimin dahil olduğunu açıklar. İstihbarat analizi, mevcut kaynakları hedeflemeye yardımcı olarak ve soruşturmaya daha net bir şekilde odaklanmak için bilgi boşluklarını belirleyerek soruşturmalara yardımcı olur. Aynı zamanda, çabaların tekrarlanmasını önlemeye ve alakasız alanlara sapmayı önlemeye yardımcı olur. Maksimum faydayı elde etmek için, bir araştırmanın mümkün olan en erken aşamasında, tercihen başlangıçta bir analiz kapasitesi kullanılmalıdır, ancak lojistik olarak bu her zaman mümkün değildir.

İSTİHBARAT DÖNGÜSÜ

İstihbarat döngüsü kavramı, genel olarak hem operasyonel hem de stratejik seviyelerde istihbarat analizi sürecinin temeli olarak kabul edilmektedir.

Şekil 2-1. istihbarat döngüsü



Yön/görev

İstihbarat analizi, müşterilerin, yani analitik ürünün tüketicilerinin ihtiyaçları tarafından yönlendirilir. Bu nedenle analitik çaba, genellikle bu müşteriler tarafından görevlendirme yoluyla yönlendirilir. Döngünün bu aşamasında inisiyatif alırlar, ancak ortaklık ilkesi, analitik ürün gereksinimlerinin her iki taraf tarafından açıkça tanımlanmasını ve anlaşılmasını sağlamak için hem kendilerinin hem de sağlayıcıların birlikte çalışma sorumluluğunu paylaşmalarını gerektirir.

İlk sorulması gereken sorular şunlardır:

" Kimin görevleri?

" Nasıl görev yapıyorlar? " Neden

görev yapıyorlar?

" Hangi görevler belirlendi?

Genel olarak bu sorular analistin oturduğu ortam içinde cevaplanacaktır ve bu nedenle bu konuda katı ve hızlı kurallar verilemez. Görevlendirmenin etkin bir şekilde işlemesi için iyi bir müşteri/analist ilişkisinin olması esastır. Analist nesnel olmalı, önyargılı fikirlerden etkilenmemeli, aynı zamanda görevi önyargısız olarak kabul etmeye istekli olmalıdır.

Görevlendirme iki temel biçimde olabilir:

Müşteri, bir konuya veya bir dizi endişe konusuna odaklanan analitik bir ürün için bir gereksinimi ifade eder .

için bir risk, tehdit veya fırsat alanıyla ilgili genel bir beklenti formüle eder.

Görev açıkça tanımlandıktan sonra, analitik birim istihbarat döngüsünün geri kalan aşamaları için kendi planlamasını başlatır.

Toplamak

İstihbarat süreci, veri elde etme ve kullanma yeteneğine dayanır. Ancak üstesinden gelinmesi gereken ilk ve en temel sorun, elektronik olarak elde edilebilirden "basılı kopyaya" kadar birçok biçimde gelen bu verilerin toplanması ve saklanmasıdır.

TOPLAMA: VERİLERİN TOPLANMASI

Bu erken aşamada, herhangi bir kurum için her zaman bir sorun olan aşırı veri yüklemesini önlemek için özen gösterilmelidir, ancak sağlayıcı, ilgili olmadığına inandığı için verilerin göz ardı edilmesi daha sonra sorunlara neden olabilir.

TOPLAMA PLANI: RESMİ OLARAK TANIMLANMIŞ BİR YAKLAŞIM
GEREKLİ BİLGİ VE ELDE ETME ARAÇLARI

İstihbarat sürecindeki tüm faaliyetlerin planlanması konusu özellikle toplama aşamasında önemlidir. Hem operasyonel hem de stratejik istihbarat analizinde, yapılacak diğer eylemler düşünülmeden önce analizin konuları ve kapsamı net olmalıdır. Gerekli bilgilerin tanımlandığı ve bunları edinme yollarının ortaya

konduğu bir toplama planı, ilgili bilgilerin düzenli ve kesin bir şekilde toplanmasını sağlamak için zorunludur.

Toplama planı, analiz için önemli olan bilgi kategorilerini, analizi yapmak için gereken belirli veri öğelerini, olası bilgi kaynaklarını ve belirli taleplerle temasa geçilecek kaynakları ve bilgilerin ne zaman ve ne zaman talep edildiğini gösteren bir çizelgeyi içermelidir. tarafından ihtiyaç duyulmaktadır. "Kaostan" kaçınmak için, analistin proaktif, hayal gücü kuvvetli ve bilgi edinmek için tüm yolları araştırdığı yapılandırılmış bir tahsilat planı yaklaşımı hayati önem taşır.

Üç ana bilgi kaynağı türü açık, kapalı ve sınıflandırılmıştır.

" *Açık kaynak (OSINT)* , halka açık olan bilgilerdir. Açık kaynak bilgilerinin çok dikkate değer bir alt kümesi "gri literatür" olarak adlandırılır. Araştırma, teknik, ekonomik raporlar, "beyaz belgeler", konferans belgeleri, tezler ve tezler, tartışma belgeleri, konuyla ilgili haber bültenleri vb. içerebilir. Bu tür kaynaklarla çalışmanın ana zorluklarından biri, mevcut bilgi olarak değerlendirmedir. Kamusal alanda sıklıkla önyargılı, yanlış veya sansasyonel olabilir.
" *Kapalı kaynak* , belirli bir amaç için toplanan ve sınırlı erişim ve genel halka açık olan bilgilerdir. Kapalı kaynak bilgileri genellikle yapılandırılmış veritabanları biçiminde bulunur. Suç istihbaratı analizi bağlamında, bu veritabanları büyük ölçüde devam eden hedefleme operasyonlarının bir parçası olarak toplanan kişisel verileri veya daha geniş sabıka kayıtlarını, araç tescil verilerini, silah ruhsatlarını vb. içerecektir.
" *Gizli* , insan ve teknik (görüntü ve sinyal istihbaratı) kaynakların kullanımı dahil olmak üzere özel olarak görevlendirilmiş gizli araçlarla toplanan bilgilerdir. Gizli bilgilerin kullanılması, genellikle yüksek doğrulukta olduğu için analitik bir ürünün kalitesini önemli ölçüde artırabilir; bununla birlikte, dağıtım üzerindeki kısıtlamalar nedeniyle analitik bir ürünü önemli ölçüde daha az eyleme geçirilebilir hale getirebilir.

İstihbarat analisti, tüm kaynak analisti olmalıdır, yani bilgi kaynaklarını erişilebilirlik veya erişim kolaylığından ziyade projeyle alakalarına göre seçmelidir. Tüm kaynaklı bir analist, yalnızca kapalı veya sınıflandırılmış veri kaynaklarının yararlı olduğu ve geçerli ve ilgili veriler içerdiği geleneksel bir kavramın kurbanı olmaktan kaçınmalıdır. Açık kaynakların kullanımı genellikle nihai ürüne ek güvenilirlik sağlar veya daha fazla kapalı veya sınıflandırılmış bilgilerin toplanmasını tetikler.

Kaynak seçimi aynı zamanda maliyet etkinliği açısından da değerlendirilebilir. Pahalı gizli varlıkları dağıtmak yerine açık kaynakların kullanılması, bir toplama çalışması için bütçeyi önemli ölçüde azaltabilir veya alternatif olarak, belirlenmiş bir bütçe dahilinde daha fazla bilgi edinilmesine izin verebilir. Açık kaynakların kullanımı ayrıca kapalı ve sınıflandırılmış bilgi kaynaklarının korunmasına veya muhafaza edilmesine yardımcı olabilir. Aynı zamanda, açık kaynakların araştırılması genellikle son derece büyük veri hacimlerinin işlenmesini gerektirdiğinden, OSINT'e dahil olan bir analist, konuyla ilgili uzmanlık eğitimi almalı veya bir OSINT uzmanı tarafından desteklenmelidir.

Bir operasyonel istihbarat analistinin nihai amacı, soruşturma altındaki suçlunun/suçluların tutuklanmasını ve/veya bir suç grubunun faaliyetlerinin kesintiye uğramasını sağlamaktır. Bu nedenle ekibin amacı, en yararlı kaynakları geliştirmek ve başarılı sonuçlar üretme olasılığı en yüksek olan bilgileri toplamak olmalıdır. Ortak bir başlangıç noktası, suçlunun ortaklarını belirlemektir; ancak amaç, ortakları kendi iyiliği için belirlemek yerine, her zaman bireyler arasındaki ilişkileri ve suç faaliyetlerindeki rollerini belirlemek olmalıdır.

Bir toplama alıştırmasında önemli bir konu kaynağın dilidir. İstihbarat analizi, çoğunlukla sınır ötesi boyutu olan organize suç faaliyetlerinin araştırılması için özellikle uygundur. Bilginin (açık kaynak bilgisi dahil) tamamen dil temelinde hariç tutulması, analitik bir ürünün kalitesi üzerinde ciddi şekilde zarar verici bir etkiye sahip olabilir. Analistlerin dil eğitimi bir çözümdür. Çeviri yazılımının kullanımı başka bir şeydir.

Bir istihbarat toplama planı aşağıdaki unsurları içerebilir:

" *Problem tanımı* — istihbarat probleminin kesin ve net bir şekilde formüle edilmesi gerekir

" *Proje amacı* — ideal olarak bir istihbarat gereksiniminin tek cümlelik tanımı

" *Proje kapsamı* — proje amacının tanımını genişletir ve analistten beklenen eylemleri belirler. Ayrıca, toplama önlemlerinin ve kaynaklarının kapsamının ve amacının ayrıntılı bir tanımını içerir.

Değerlendirme

Bir çıkarımın geçerliliği, çıkarımın arkasındaki verilerin kalitesiyle doğrudan bağlantılıdır. Bu nedenle veri değerlendirmesi, istihbarat döngüsünün önemli bir unsurudur. Değerlendirmenin bilginin edinildiği bağlamda gerçekleşmesini sağlamak için (yerel bir ortamda doğru bir şekilde sunulmamış bilgiyi değerlendirmek zor olduğundan) elde edilmesiyle aynı anda veya hemen ardından yapılmalıdır. Değerlendirme, kaynağın (bilginin sağlayıcısı) güvenilirliğinin ve bilgilerin geçerliliği ve doğruluğunun ayrı bir değerlendirmesini gerektirir.

DEĞERLENDİRME: KAYNAĞIN GÜVENİLİRLİĞİNİN DEĞERLENDİRİLMESİ VE BİLGİ KALİTESİ

Kaynak ve asıl bilgi birbirinden bağımsız olarak değerlendirilmelidir ve bu nedenle raporu dolduran kişinin değerlendirme sistemi hakkında sağlam bir bilgiye sahip olması zorunludur. En yaygın olarak kullanılan iki sistem 4 x 4 ve 6 x 6'dır (Bu temel sürecin daha fazla ayrıntısı için bkz. bölüm 4 "Kaynak ve verilerin değerlendirilmesi").

harmanlama

Harmanlama, toplanan bilgilerin ve/veya istihbaratın hızlı ve doğru erişime izin veren yapılandırılmış (dizinlenmiş, çapraz referanslı) bir biçimde bir depolama sistemine (dosya dolabı veya bilgisayarlı veri tabanı) aktarılmasıdır. Toplama sırasında elde edilen her bilgi veya belgenin toplu olarak dosyalanmasıyla eşdeğer değildir. Alakasız, yanlış ve başka türlü işe yaramaz bilgiler ayıklanır.

HARMANLAMA: TOPLANAN VERİLERİN, ELDE EDİLEBİLECEK VE ANALİZ EDİLECEK BİR FORMATTA ORGANİZASYONU

Veri entegrasyonu ve analizi

İstihbarat sürecinin analiz aşaması kilit bir aşamadır. Analiz, mevcut bilgilerin anlamının ve temel özelliklerinin derinlemesine incelenmesi olarak tanımlanabilir. Analiz, bilgi boşluklarını, güçlü ve zayıf yönleri vurgular ve ileriye dönük yollar önerir.

ANALİZ: BİLGİLERİNİ KEŞFETMEK İÇİN BİLGİLERİN DİKKATLİ İNCELENMESİ ANLAMI VE TEMEL ÖZELLİKLER

Analitik süreç, hem kısa vadeli operasyonel amaçlar hem de uzun vadeli stratejik nedenlerle kanun uygulama hedeflerini yönlendirmek için istihbaratın kullanılmasını ve geliştirilmesini amaçlar. Analizin kapsamı ve genel güvenilirliği, analistin becerileriyle birlikte edinilen bilgilerin düzeyine ve doğruluğuna bağlıdır. Analiz, her tür yasa uygulama hedefine yardımcı olmak için gerçekleştirilebilen döngüsel bir süreçtir. Farklı suç türleri ve suç operasyonları farklı senaryolar gerektirir, ancak her durumda kullanılan bilgiler yapay ve keyfi olarak dayatılan seçici bir ızgara aracılığıyla önceden filtrelenmemelidir.

Veri entegrasyonu, analitik sürecin ilk aşamasıdır. Çıkarımların formülasyonu için hazırlanırken farklı kaynaklardan gelen bilgileri birleştirmeyi içerir. Bu bilgiyi görüntülemek için çeşitli teknikler kullanılabilir, en yaygını grafik tekniklerinin kullanılmasıdır.

- *Bağlantı şeması* —araştırmada yer alan varlıklar arasındaki ilişkileri göstermek için
- *Olay grafiği* — varlıklar veya olay dizileri arasındaki kronolojik ilişkileri göstermek için
- *Emtia akış şeması* - para, narkotik, çalıntı mal veya diğer emtia hareketlerini keşfetmek için
- *Faaliyet çizelgesi* — bir suç operasyonunda yer alan faaliyetleri belirlemek için
- *Finansal profil oluşturma* — bireylerin veya ticari kuruluşların gizli gelirlerini belirlemek ve ekonomik suç göstergelerini belirlemek için
- *Frekans çizelgesi* — nicel bilgileri düzenlemek, özetlemek ve yorumlamak için
- *Veri korelasyonu* — farklı değişkenler arasındaki ilişkileri göstermek için

Analitik süreçteki bir sonraki adım, gerçeklerin ötesine geçmeyi gerektiren yorumlama veya mantıksal akıl yürütmedir. Disiplinli analiz yaklaşımı, alaka düzeyini belirlemek için entegrasyon sırasında değerlendirilecek maksimum miktarda bilgiyi gerektirir. Sürecin başındaki bilgileri hariç tutmak, hayati bir bilgi parçasının kolayca gözden kaçırılmasına neden olabilir. Bu, sonuçta bir soruşturmayı tehlikeye atabilecek yanlış analize yol açabilir.

Analiz genellikle orijinal projeye teğet olan ek projeleri tanımlar. Geçmişte, bu projeleri ana proje ile birlikte ve aynı anda üstlenmek olağandı. Bu yaklaşım, kaynakların dağılmasına, gecikmelere ve nihai ürün(ler)de genel olarak daha düşük kaliteye yol açtı. Deneyim yoluyla, analitik projelerin sırayla, birer birer veya bağımsız analist ekipleri tarafından üstlenilmesi gerektiği artık kabul edilmiştir.

Bağlantı analizi gibi veri tanımlama ve entegrasyon teknikleri kendi başlarına bir amaç değildir. Bunlar, bilgiden anlam türetme sürecinde analistler tarafından kullanılan basit araçlardır. İlk gerçek analitik ürün bir çıkarımdır. Öncüllerden bir çıkarım gelir; yaygın bir hata, sezgisel olarak bir çıkarım geliştirmek ve ardından onu destekleyecek öncüller aramaktır. Öncüllerin önceliğine yapılan bu vurgu, "çıkarımı destekleyen öncüller…" değil, "Beni çıkarımıma götüren öncüller…" gibi bir ifadeyle tekrarlanmalıdır (Ancak sonuçları sunarken, çıkış noktası çıkarımdır—büyük fikir—ve ardından geldiği öncüller).

Çıkarım geliştirmede bir "öncül", belirli bir noktaya değinmek için bir araya gelen gerçekleri veya bilgi parçalarını tanımlamak için kullanılır. Binalar, veri açıklamasına kıyasla gerçek veri analizi sürecindeki ilk ve kilit aşamadır. Öncüllerin nasıl tanımlandığını anlamak, çıkarımlar geliştirmek için çok önemlidir.

Binalar, açıklanan bilgilere en yakın bağlantıdır ve bu nedenle verilerin en objektif ve doğru temsilidir. Belirli bir bilgi dizisinden türetilen herhangi bir öncül seti için, öncüller farklı çıkarımlar önermek için farklı şekillerde birleştirilebilir.

Dört tür çıkarım vardır:

" *Hipotez* — geçici bir açıklama, doğrulama veya reddetme için ek bilgi gerektiren bir teori.
" *Tahmin* — gelecekte olacak bir şey hakkında bir çıkarım.
" *Tahmin* — bir örnekten bütün hakkında yapılan, tipik olarak nicel nitelikte bir çıkarım.

" *Sonuç* — iyi desteklenen bir açıklama.

Tüm çıkarımların, gerçek olarak kabul edilmeden önce bir şekilde test edilmesi gerektiğine dikkat edilmelidir.

yaygınlaştırma

Bir istihbarat analisti, analitik ürünleri uygun şekilde hedeflenen kitlelere yayma sorumluluğuna sahiptir. Rutin dağıtımın çoğu kısa notlar yoluyla yapılabilir. Ancak istihbarat analistleri, daha büyük soruşturmalar hakkında sözlü brifing verebilmeli ve mevcut bilgileri detaylandıran yapılandırılmış raporlar yazabilmelidir.

YAYGINLAŞTIRMA: ANALİZ SONUÇLARININ MÜŞTERİYE AÇIKLANMASI

Tüm süreç boyunca, müşteri analistle yakın istişare içinde olacak ve belirli bir projeyle ilgili soruları yanıtlaması için çok sayıda fırsat istenecekti.

Yaygınlaştırma süreci aşağıdakiler gibi çeşitli biçimlerde olabilir:

" Yapılandırılmış resmi raporlar

Destekleyici belgelerle birlikte yapılandırılmış ve resmi sözlü sunumlar

şeklinde haftalık genel bakış

" İstihbarat ve soruşturma ekiplerine geçici brifing

Yaygınlaştırma aşaması, istihbarat sürecinin ilk döngüsünü tamamlar.

yeniden değerlendirme

Yeniden değerlendirme, döngünün herhangi bir aşamasının iyileştirilebileceği yolları belirlemek için tüm istihbarat döngüsünün sürekli olarak gözden geçirilmesini içerir. En değerli olması için, yeniden değerlendirme sadece döngünün son aşamasına bırakılmamalı, süreç boyunca yapılmalıdır. Yeniden değerlendirme şu adrese yönlendirilebilir:

" süreç

" Analitik ürün

" Analitik ürünün kullanımı

" Raporlamanın etkinliği

" Personel dağıtımı

" Öncelik ayarı

" Analistin bakış açısı

" Müşterinin bakış açısı

İstihbarat faaliyeti, bir kişinin veya bir grup insanın bireysel girişimciler olarak yaptığı bir şeyin aksine, kolektif bir süreçtir.

3. Ulusal istihbarat modeli örneği: Birleşik Krallık

Birleşik Krallık'ın Ulusal İstihbarat Modeli (NIM) iki öncül üzerine kuruludur:

1. Birleşik Krallık'ta üç suç düzeyi vardır: tek yargı alanı, çok yargı alanı ve uluslararası.

Bunlar, suç faaliyetlerini üç düzeyde etkilemek üzere tasarlanmıştır:

" *Düzey 1—Yerel sorunlar*— genellikle suçlar, suçlular ve temel bir komuta birimini veya küçük bir kuvvet alanını etkileyen diğer sorunlar. Suçların kapsamı, değeri düşük hırsızlıktan cinayete kadar geniş bir yelpazede olacak. Hacim suçlarının ele alınması bu düzeyde özel bir konu olacaktır.

" *Seviye 2—Sınır ötesi sorunlar*— genellikle bir suçlunun eylemleri veya birden fazla temel komuta birimini etkileyen diğer özel problemler. Anahtar konular, ortak sorunların belirlenmesi, uygun verilerin değişimi ve ortak yarar için kaynakların sağlanması olacaktır.

" *Seviye 3—Ciddi ve organize suç* — genellikle ulusal ve uluslararası ölçekte faaliyet gösteren, proaktif araçlarla tanımlama ve öncelikli olarak özel birimler tarafından hedeflenen operasyonlar ve ulusal bazda önleyici müdahale yoluyla müdahale gerektiren.

2. Kolluk kuvvetlerinin arzu edilen sonuçları şunlardır: toplum güvenliği, suç azaltma, cezai kontrol ve düzensizlik kontrolü. Model bunu, suçu, suçluları, düzensizliği ve sorunları yönetme işinden, toplum güvenliğinin istenen sonuçlarına, suçun azaltılmasına ve kontrollü suçluluğa geçme hedefine ulaşmak için temel olan dört ana bileşen aracılığıyla başarır:

" Görevlendirme ve koordinasyon süreci

" Dört temel istihbarat ürünü

" Bilgi ürünleri " Sistem ürünleri.

Görevlendirme ve koordinasyon süreci

Görevlendirme ve koordinasyon grubu toplantılarına , gerekli kaynakları yerleştirme yetkisine sahip olan ve kolluk kuvvetlerinin planlanması ve yürütülmesi için temel işlevsel sorumluluğa sahip kişilerden oluşan bir komuta biriminin üst düzey yöneticisi başkanlık eder.

Stratejik görevlendirme , kontrol stratejisini (yani istihbarat, önleme ve uygulama öncelikleri) oluşturmayı veya değiştirmeyi ve öncelikleri belirledikten sonra ana kaynak taahhütlerini yapmayı amaçlar.

Taktik görevlendirme , *kontrol stratejisine taktik menüyü* devreye almayı ve uygulamayı, yeni ihtiyaçlara yanıt vermeyi ve üzerinde anlaşmaya varılan planların uygulanmasının izlenmesini amaçlar. *Taktik menü* dört unsurdan oluşur :

" *Kontrol stratejisinin* öncelikleri doğrultusunda suçluları hedef almak ;

" Suç ve düzensizlik sıcak noktalarının yönetimi;

" Seri" ile bağlantılı olduğu gösterilebilecek suç ve olayların soruşturulması;

Kapalı devre televizyon (CCTV) ve aydınlatma şemaları veya topluluk eylemi girişimleri gibi bir dizi "önleyici tedbirin" uygulanması .

İstihbarat ürünlerinin üretimi—istihbarat ürünlerinin yaratılması, istihbarat kabiliyeti için harekete geçen görev ve koordinasyon grubundan kaynaklara ve yönlendirmeye aynı bağlılığı gerektirir.

Anahtar istihbarat ürünleri, istihbarata dayalı polisliğin uygulanabileceği ve etkisinin suçun azaltılması, tutuklamalar, kesintiler ve artırılmış toplum güvenliği açısından ölçülebileceği "çıktılar"dır. İstihbarat ürünleri, ham bilgilerin toplandığı, analiz edildiği ve yorumlandığı ve gerekli kararlar veya eylem seçenekleri hakkında tavsiyelerle temsil edildiği analistler ve istihbarat görevlileri arasındaki işbirliğinin sonucudur. Kolluk kuvvetlerine istihbarat odaklı yaklaşım, aşağıdaki tablo 3-1'de gösterildiği gibi yalnızca dört geniş istihbarat ürünü sınıfını gerektirir:

Tablo 3-1. Dört istihbarat ürünü kategorisi

Ürün	Amaç	Amaç	Tanım
.Strategicassessment	Bir alandaki uzun vadeli sorunları, kapsamını ve suçluluktaki büyüme tahminlerini belirlemek.	Kolluk kuvvetleri önceliklerini belirlemek, kaynak tahsislerini belirlemek, iş planlamasını desteklemek ve üst düzey yöneticileri ve politika yapıcıları bilgilendirmek; Bir kontrol stratejisi belirlemek için: istihbarat için öncelikler, önleme ve uygulama.	" Amaç (referans şartları) Kapsam (fonksiyonel/coğrafi) Mevcut durum/anket Belirlenen/karşılanan ana hedefler " Son değerlendirmeden bu yana ilerleme " Başlıca suç alanları Demografik/sosyal sorunlar " Desenler / trendler " Kaynak kısıtlamaları (genel bakış/özet)
.Tacticalassessment	Bir alandaki daha kısa vadeli sorunları belirlemek için bu, hızlı eylemle bir durumun kötüleşmesini veya gelişmesini engelleyebilir. "Taktik menüsünde" mevcut işlerdeki ilerlemeyi izlemek için.	Mevcut operasyonların ve planların yönetimine yardımcı olmak, kaynakları ve çabaları değişen ihtiyaç ve sorunlara göre yeniden tahsis etmek.	Mevcut durum—hedeflemede ilerleme; suç ve diğer seriler; sıcak noktalar; önleyici tedbirler " Daha fazla eylem için seçenekler Avantajlar/dezavantajlar. En iyi hareket tarzı " Zaman çerçevesi (kısa/orta) " Kaynak etkileri/değişiklikleri

Ürün	Amaç	Amaç	Tanım
.Targetprofile	Müteakip eylem için (potansiyel) suçlunun ve ortaklarının ayrıntılı bir resmini sağlamak.	Operasyonel yönetime hedefleri seçmede, araştırmaları yönlendirmede, planları şekillendirmede ve gözetimi sürdürmede yardımcı olmak.	"Kişisel kayıt" Adli sicil kaydı "Finansal profil " Ağ/ilişkilendirme raporu "İletişim raporu "Ulaştırma raporu " Gözetim değerlendirmesi "İstihbarat boşlukları
.Problemprofile	Yerleşik ve ortaya çıkan suç/olay serilerini ve suç sıcak noktalarını belirlemek.	Soruşturma ihtiyaçlarının kaynaklanması, hedefleme, sıcak nokta yönetimi, suç azaltma girişimlerinin yönlendirilmesi ve suç önleme tedbirleri konusunda yönetime yardımcı olmak.	" Sorun tanımlama " Arka plan ve nedenler " Hasar ölçeği " Bozukluk/suç işleme düzeyi " failler " İç/dış bağlantılar " Sosyal etki "Kaynak etkileri

İstihbarat çalışmasının önceliklendirilmesi — görevlendirme ve koordinasyon grubunun önemli bir sorumluluğu istihbarat kabiliyetine kaynak sağlamak, yönlendirmek ve sürdürmektir. İstihbarat çalışmasının tamamen etkili olması için, istihbarat faaliyetlerinin belirlenen stratejik ve taktik öncelikleri takip etmesini sağlayan yeterli varlıklara (kaynaklar, insanlar, bilgi ürünleri, sistem ürünleri) ve disiplinlere ihtiyacı vardır.

Bilgi kaynakları, reaktif veya proaktif çalışma ile sınırlandırılmamalıdır. Mevcut reaktif çalışmanın sonuçları içinde çok değerli veriler mevcuttur. Yeterli bir proaktif yetenek de önemlidir.

Belirli roller için doğru insanlara yatırım yapmak önemli bir faydadır. İşin üç ana bileşeni vardır: veri yönetimi, analiz ve özel istihbarat toplama. İstihbarat yöneticisi, komuta biriminin işini, istihbarat toplama ve analizini bir araya getirmek için gerekli katalizördür. Tüm istihbarat çalışmaları bilgi ve sistem ürünleri ile desteklenmelidir.

Bilgi ürünleri

Bunlar, vasıflı süreçlerin tamamlandığı ve ajanslar arasında çalışmanın hangi koşullar altında gerçekleşebileceğine ilişkin iş veya en iyi uygulamaların yürütülmesine ilişkin kuralları tanımlayan yerel veya ulusal bir dizi ürünü temsil eder. "Bilgi ürünleri" yaklaşımı aynı zamanda, personel konularının kolluk kuvvetleri için daha profesyonel temelli bir istihbarat rejimine taşınmasında boşluk analizini yönetmenin de yararlı bir yolunu temsil eder.

" Milli istihbarat modeli

" Veri koruma yönergeleri

" Uygulama kuralları

" Ulusal kılavuzlar ve standartlar:

- İstihbaratın kaydedilmesi ve yayılması
- Gözetim
- Gizli operasyonlar ve test satın alımları - Muhbirlerin kullanımı
- Müdahale ve iletişimle ilgili verilere erişim—- Gizli teknikler hakkında içtihat
- Yerel araştırma ve veri erişim protokolleri
- Yerel kurumlar arası erişim protokolleri - İstihbarat eğitimi

Sistem ürünleri

Sistem ürünleri, bilgilerin toplanmasını, alınmasını, kaydedilmesini, depolanmasını, kullanılmasını ve yayılmasını sağlar. Genel olarak, üç türe ayrılabilirler:

" *Araştırma süreci sırasında veri depolama, geri alma ve karşılaştırma araçlarına* erişimin sağlanması, büyük miktarlarda hazır kolluk kuvvetlerine ve diğer ilgili verilere erişim, istihbarata dayalı polisliğin bel kemiğidir. Ülke çapındaki sistemlerin daha yerel ve uzmanlaşmış sistemlerle birleştirilmesi, cezai ve diğer sorunların karmaşık analizi için muazzam bir potansiyel sağlar. Analiz edilen istihbarat ürünlerinin kalitesi açısından başarının anahtarı, farklı IS platformlarından gelen verilere erişme ve bunları bir araya getirme yeteneğidir. Aşağıdakileri içeren çeşitli bilgisayarlı sistemleri içerebilirler:

- Suç kayıtları
- Açık kaynak verileri
- istihbarat dosyaları
- Analiz araçları
- Özel veri tabanları (örneğin, ateşli silahlar kaydı, sürücü ehliyeti, sabıka kayıtları vb.) - Vaka yönetimi araçları.

" *Yeni bilgi ve istihbarat elde etmek için tesislere veya sistemlere erişimin sağlanması* —belirlenen ihtiyaçların karşılanması için istihbaratın toplanması, "insan muhbirler veya gizli görevliler gibi kaynaklar veya insan veya teknik gözetim kaynaklarının konuşlandırılması. Daha yüksek operasyon seviyelerinde, karmaşık gizli giriş tekniklerine erişim veya iletişimleri engelleme gerekliliği olacaktır. Daha müdahaleci teknikler genellikle yalnızca ciddi suç vakalarında mevcuttur ve metodolojilerin gizliliğini koruma gerekliliği, bu şekilde uygulanamayacakları yerlerde kullanılmalarını istenmeyen hale getirir. Mobil gözetim kaynakları genellikle pahalıdır ve konuşlandırılmaları için sağlam bir istihbarat vakasının oluşturulmasını gerektirir.

Yerel düzeyde, istihbarat birimleri, o düzeyde yürütülen soruşturmalarla orantılı teknik gözetim tesislerine ve ihtiyaç duyulduğunda daha karmaşık tesislere erişilebilecek açık sistemlere sahip olmayı

gerektirecektir. Polis güçleri içinde, gözetleme kaynaklarının dağıtımı ve daha pahalı veya hassas erişim sistemleri, suç ve istihbarat stratejilerinin ayrılmaz bir parçası olacak politika konuları olacaktır.

" *Operasyonel güvenlik sistemlerinin sağlanması*— istihbarat değerli bir metadır ve bu nedenle dikkatle ele alınmalıdır. "Bilmesi gereken" ilkesi, istihbarat doktrininin bel kemiği olarak yaygın olarak kabul edilmektedir.

Potansiyel faydasını en üst düzeye çıkarmak için bilgiyi mümkün olduğunca geniş bir şekilde erişilebilir kılmak ile kaynakların, tekniklerin ve bilgilerin güvenliğini korumak için erişilebilirliğini kısıtlamak arasında kurulacak doğru denge çok önemlidir. Bir dizi erişim sistemi ve tesisi, istihbarat ortamının bütünlüğünü ve etkinliğini desteklemeye yardımcı olur:

- Bilgilendirici kayıt sistemi;
- Doğru standardın analitik araçlarının sağlanması ve kullanılması;
- Güvenli konaklama ve güvenli depolama tesislerinin sağlanması;
- Gerektiğinde uygun şekilde güvenli, uygun brifing olanaklarının sağlanması;
- Risk değerlendirmesi ve işleme kısıtlamalarını içerebilen ulusal bir standart istihbarat kayıt formunun benimsenmesi;
- Yabancı kolluk kuvvetlerine kontrollü erişim.

Analitik teknikler ve ürünler

Ulusal İstihbarat Modeli, daha önce tartışıldığı gibi dört temel istihbarat ürününe dayanmaktadır. Bu ürünler de, etkin proaktif kanun uygulama tekniklerinde mesleki bilginin gelişimini destekleyen dokuz analitik teknik ve üründen türetilmiştir.

Tablo 3-2. Dokuz çeşit analitik teknik

Ürün	Tanım	Amaç
.Resultsanalysis	Aşağıdakilerin etkisini değerlendirir: " Devriye stratejileri ve taktikleri "Reaktif soruşturmalar "Proaktif soruşturma " Suç azaltma girişimleri " Diğer kolluk kuvvetleri politikaları ve teknikleri	" En iyi uygulamayı belirlemeye yardımcı olmak "İyileştirme alanları Mesleki gelişime yardımcı olarak olayların ve soruşturmaların post hoc brifingi

.Crimepatternanalysis	" Suç dizisi tanımlama " Suç eğilimi tespiti "Sıcak nokta analizi " Genel profil analizi	Aşağıdakilerin "taktik menüsü" içinde önceliklendirme ile ilgili yönetim kararları: "Sıcak noktalar " Suç dizisi tanımlamaları " Suç ve düzensizliği önleme ve yönlendirme girişimleri Operasyonel olarak, daha fazla analiz için yeni ve ortaya çıkan eğilimleri ve gereksinimleri belirlemede araştırmacılara ve diğerlerine yardımcı olurlar.

Ürün	Tanım	Amaç
.Marketprofiles	Bir mal veya hizmet (uyuşturucu, çalıntı araçlar, fuhuş vb.) " Anahtar oyuncular " ağlar " Suç malları Suçluluktaki ilişkili eğilimler Bu profiller, esas olarak ağ ve suç modeli analizinden elde edilen diğer analitik ürünlerden oluşur.	Cezai ve yaptırım sorunlarının önceliklendirilmesine ilişkin yönetim kararları – hedeflerin ve azaltma fırsatlarının belirlenmesi: Yerel olarak tutulan standart piyasa profillerinin bir araya getirilmesi, daha üst düzey bir görünümün oluşturulmasını sağlar. Profil, operasyonları desteklemek için hedef profillerde daha ayrıntılı analizi, suç kalıbı analizini veya ağ analizini tetikleyebilir.
.Demographic/social trendsanalysis	Demografik değişikliklerin doğası Suçluluk veya görünüşe göre bağlantılı suçluluk üzerindeki etkisi Suçlulardaki veya kusurlu davranışlardaki değişikliklerin veya eğilimlerin altında yatan sosyal faktörlerin daha derin analizi Bilinen veya tahmin edilen sosyal veya demografik değişikliklere yönelik bir suç ve düzensizlik denetimi veya araştırmasını destekleyebilir.	"Kanun uygulamasında kaynak bulma ve öncelikler hakkında stratejik kararlar " Gelecekteki baskıların muhtemel olduğu yerleri aydınlatır ve ortakları bilgilendirir " Ortaya çıkan sosyal fenomenlere veya insan hareketlerine yanıt olarak mevsimsel veya diğer taktik operasyonların planlanmasında kullanım
.Criminalbusinessprofiles	Aşağıdakileri içeren ayrıntılı operasyonel modaliteyi ortaya çıkarır: " Kurbanlar nasıl seçilir? Suçlular tarafından kullanılan teknik uzmanlık Suçlular tarafından istismar edilen sistem veya prosedürlerdeki zayıflık " Diğer analiz türlerinden elde edilen sonuçları içerir	Aşağıdaki değişiklikler için ihtiyaçların vurgulanması: " Mevzuat veya diğer düzenleme biçimleri " Yeni tehditleri karşılamak için kaynak sağlama Kesinti için kilit noktaların belirlenmesinde operasyonel planlama " Derhal suç önleme/azaltma fırsatları

		" Eğitim ve brifing ürünleriyle bilgi standartlarını yükseltmek
.Networkanalysis	" Ağ içindeki bireylerin temel özellikleri ve işlevleri " Ağ içindeki/dışındaki dernekler " Ağın güçlü ve zayıf yönleri " Mali ve iletişim verilerinin analizi Hedef profillerle bağlantılı olarak suç davranışı hakkında çıkarımlar	*Stratejik olarak:* Stratejik mülahazalar için bağlantılı suçluluğun ciddiyetini yönetime göstermek *Taktik ve operasyonel olarak:* " Hedef operasyonları bilgilendirir Etkili sorgulama hatları ve kesinti için fırsatlar önerir Kaynak dağıtımlarını yönlendirmek için istihbarattaki boşlukları vurgular
.Riskanalysis	Bireysel suçlular veya kuruluşlar tarafından aşağıdakilere yönelik karşılaştırmalı risklerin analizi: "Bireysel potansiyel kurbanlar "Kamuoyunun geneli " Kolluk	Hem stratejik hem de operasyonel seviyelerde istihbarat veya uygulama çalışmalarına öncelik verilmesi için bir başlangıç olarak risk değerlendirmelerinin derlenmesi, risk yönetimi planlarının tamamlanmasına yol açar.

Ürün	Tanım	Amaç
.Targetprofileanalysis	Suç kapasitesini aydınlatır ve aşağıdakiler hakkında bilgi içerir: " dernekler " Yaşam tarzı "Operasyonel modalite " Finansal Veri "Güçlü ve zayıf yönler Geçmişte hedefe karşı işe yarayan veya başarısız olan teknikler Tamamen "suç" faaliyeti ile sınırlı olmamak üzere, her türlü suç teşkil eden faaliyeti kapsayabilir	Hedef operasyonları şu şekilde destekleyin: " Hedef seçimi bilgilendirme İstihbarat ihtiyaçlarının belirlenmesi " Kaynakların ve kaynakların hedefe karşı nasıl konuşlandırılabileceğini gösteren

.Operationalintel - ligenceassessment research	Gerçek zamanlı değerlendirme ve araştırma: "Dernekler hakkında gelen bilgiler Mevcut bir operasyonda şüphelilerin etrafındaki diğer fenomenler Tamamen bir analistin sorumluluğunda olabilir veya olmayabilir.	"Görev kaymasının" önlenmesi ve mevcut bir operasyon sırasında gelen istihbarattan kaynaklanan araştırma ihtiyaçlarının önceliklendirilmesi ve devam eden istihbarat çalışması için ortaya çıkan önceliklerin belirlenmesi.

4. Kaynak ve verilerin değerlendirilmesi

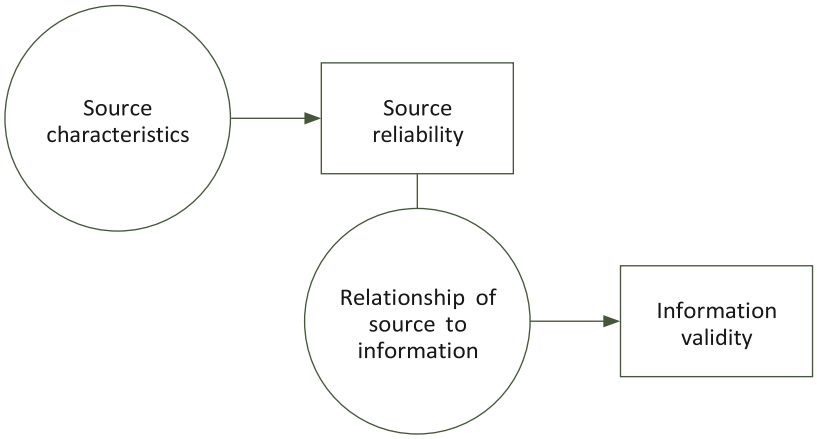
KAYNAK VE BİLGİLERİN DEĞERLENDİRİLMESİ

Bilgi toplandıktan sonra, genellikle göz ardı edilebilecek geleneksel kanun uygulama faaliyetinde bir aşama olarak değerlendirilmelidir. Tam ve doğru bir değerlendirme, kaynağın güvenilirliğinin ve bilginin geçerliliğinin değerlendirilmesini gerektirir. Bu aşama, bir bütün olarak istihbarat süreci için çok önemlidir ve bu nedenle kendi başına açıklayıcı bir bölüm gerektirir.

4 x 4 sistemi olarak bilinen ve şu anda kolluk kuvvetleri için yaygın bir uygulama olarak kabul edilen sistem kullanılarak standartlaştırılmış bir değerlendirme sistemi geliştirilmiştir. Bu sistem örneğin Europol'deki analistler tarafından kullanılmaktadır ve Europol'de alınan ve değerlendirilmeyen herhangi bir bilgi kullanımdan önce bu sisteme göre değerlendirilecektir.

Diğer kurumlar bu sistemin varyantlarını kullanır, ancak her biri açıklayıcı tablolara referansla kolayca yorumlanabilir ve gerekirse bilgiler bir sistemden diğerine dönüştürülebilir.

Şekil 4-1. değerlendirme süreci



Değerlendirme için üç temel ilke geçerlidir:

1. Kişisel duygulardan etkilenmemeli, profesyonel yargıya dayanmalıdır.
2. Kaynağın değerlendirilmesi bilgiye ayrı ayrı yapılmalıdır.
3. Mümkün olduğunca kaynağa yakın yapılmalıdır.

4 x 4 sistemi kullanan değerlendirme tabloları

Tablo 4-1. Kaynak değerlendirmesi

A	" Özgünlük, güvenilirlik, bütünlük, yeterlilik veya "Tam güvenilirlik tarihi

B	" Bilginin alındığı kaynağın çoğu durumda güvenilir olduğu kanıtlanmıştır.
C	" Bilginin alındığı kaynağın çoğu durumda güvenilmez olduğu kanıtlanmıştır.
X	"Güvenilirlik yargılanamaz

Tablo 4-2. Bilgi değerlendirmesi

1	"Doğruluk konusunda şüphe yok
2	" Kaynağa kişisel olarak bilinen, ancak aktaran yetkiliye kişisel olarak bilinmeyen bilgiler "Kendi içinde mantıklı " Konuyla ilgili diğer bilgilerle aynı fikirde
3	"Kaynağında kişisel olarak bilinmeyen ancak daha önce kaydedilmiş diğer bilgilerle doğrulanan bilgiler
4	"Kaynağında kişisel olarak bilinmeyen ve bağımsız olarak doğrulanamayan bilgiler

6 x 6 sistemi kullanan değerlendirme tabloları

Tablo 4-3. Kaynak güvenilirliği

A TAMAMEN GÜVENİLİR	" Özgünlük, güvenilirlik, bütünlük, yeterlilik konusunda şüphe yok "Tam güvenilirlik tarihi
B GENELLİKLE GÜVENİLİR	" Özgünlük veya güvenilirlik veya bütünlük veya yeterlilik konusunda bazı şüpheler (bir sayı) " Genel güvenilirliğin tarihi
C ADİL BİR ŞEKİLDE GÜVENİLİR	" Özgünlük, güvenilirlik, dürüstlük, yeterlilik konusunda şüphe (iki sayı ve daha fazlası) " Periyodik güvenilirliğin tarihi
D GENELLİKLE GÜVENİLİR DEĞİLDİR	" Özgünlük, güvenilirlik, dürüstlük, yeterlilik konusunda kesin şüphe Ara sıra güvenilirliğin tarihi
GÜVENilmez	" Özgünlük, güvenilirlik, bütünlük, yeterlilik eksikliği hakkında kesinlik "Güvenilmezliğin tarihi
F	"Yargılanamaz

Tablo 4-4. Veri geçerliliği

1 ONAYLANDI	" Diğer bağımsız kaynaklar tarafından doğrulandı "Kendi içinde mantıklı " Konuyla ilgili diğer bilgilerle aynı fikirde

2 **MUHTEMELEN DOĞRU**	" Bağımsız olarak doğrulanmadı "Kendi içinde mantıklı " Konuyla ilgili diğer bilgilerle aynı fikirde
3 **OLASI DOĞRU**	" Onaylanmadı "Kendi içinde mantıklı " Konuyla ilgili diğer bilgilerle biraz aynı fikirde
4 **KESİNLİKLE DOĞRU**	" Onaylanmadı "Mantıksız değil " Makbuz sırasında mümkün olmasına rağmen inanılmıyor
5 **İMKANSIZ**	" Aksini teyit etmek mümkün "Kendi içinde mantıksız " Konuyla ilgili diğer bilgilerle çelişiyor
6	"Yargılanamaz

Yukarıdaki iki değerlendirme sisteminin, özellikle bilginin değerlendirilmesi söz konusu olduğunda, sadece not sayısından daha fazla farklılık gösterdiği açıktır. 4 x 4 sistemi basit bir kişisel bilgi kavramına dayanmaktadır. Kulaktan dolma bilgilere daha düşük bir puan verilir. Bu basitlik, değerlendirme daha az öznel hale geldiğinden, kendi içinde bir değere sahiptir.

sanitasyon

Değerlendirmenin ardından, bir sanitizasyon sistemi ile devam edilmesi tavsiye edilir. Bunun amacı, bilginin kaynağının veya kaynağının, raporun içeriğinden veya ifadesinden tespit edilebilir olmaktan korunmasıdır. Ayrıca istihbaratın elde edildiği koşulları veya yöntemi korumaya da çalışır. Bu sürece yardımcı olmak için en iyi uygulama örnekleri olarak aşağıdaki sanitizasyon yönergeleri sunulmaktadır:

" Tüm istihbarat doğru bir şekilde kaydedilmelidir. Yaygınlaştırma raporları, yalnızca yayımın istenen amacına ilişkin istihbaratı içermelidir;

" Herhangi bir şekilde kaynağı tanımlayan tüm materyallerin metinden çıkarılmasına özen gösterilmelidir;

" İnsan kaynaklarıyla yapılan toplantıların zamanlaması ve yeri alakasız olabilir ve kaynağın tanımlanmasına yol açabilir;

" Aynı kaynaktan tekrarlanan istihbarat, kaynağın tanımlanmasına yol açabilir. Referans numaralarının rastgele tahsis edildiği gizli bir kaynak kaydının kullanılması bu olasılığı azaltır;

" Temizlik, okuyucunun kaynağın insan mı yoksa teknik mi olduğunu belirlemesini imkansız hale getirmelidir;

" Bazı durumlarda, bir kaynağın gerçek kimliğini, kaynak olarak kimliğini açıklamadan istihbarat gövdesinde ortaya çıkarmak avantajlı olabilir. Bu, örneğin bir kaynak diğer görevliler veya suçlular tarafından grupla birlikte görüldüğünde gerekli olabilir.
adı geçen kişiler ve raporda kaynağın adının verilmemesi, kimliği hakkında şüphe uyandırabilir;

" Bazen tek bir raporun istihbaratı, sadece sınırlı sayıda bireyler tarafından bilinebilecek bir dizi istihbarat materyali içerecektir. Bu materyali parçalara ayırın.

daha fazla güvenlik sağlamak için birden çok rapor ve gizli bir kaynak kaydından farklı referanslar atama;

Bir memurun, bir raporun içeriğinin kaynağı gösterebileceğinden endişe duyması halinde, bir istihbaratın yayımlanmasından veya bir istihbarata girmesinden önce bir amirine atıfta bulunulmalıdır.

sistem gerçekleşir.

yaygınlaştırma

Bu aşamada tamamlanması gereken diğer bir süreç, herhangi bir alıcıya bilgi ile ne yapabilecekleri konusunda rehberlik etmektir. Bu, ya rapora bir güvenlik sınıflandırması atayarak (ör. gizli, gizli, kısıtlı) ya da kimin hakkı veya verilmesi gerektiğini belirleyen bir dizi izin ve kısıtlama olan bir "işleme kodu" tahsis ederek yapılabilir. erişim.

Aşağıda, kod işleme sistemine bir örnek verilmiştir:

Tablo 4-5. İşleme kodları

1	Menşe ülkedeki kolluk kuvvetleri içinde yayınlanmasına izin verilir.
2	Diğer ulusal ajanslara yayılmasına izin verilir.
3	Uluslararası kolluk kuvvetlerine dağıtılmasına izin verilir.
4	Yalnızca kaynak kuruluş içinde yayma.
5	Yayına izin verir, ancak alıcı kuruluş belirtilen koşullara uymak zorundadır.

Bu tür işleme kodları, daha önce kaynak ve bilgiye tahsis edilen kodlara eklenebilir. Böylece bir B24 kodu şu şekilde çevrilir:

B— Bilginin alındığı kaynağın çoğu durumda güvenilir olduğu kanıtlanmıştır.

2- Kaynağa kişisel olarak bilinen, ancak aktaran kişinin kişisel olarak bilmediği bilgiler

4—Yalnızca kaynak kuruluş içinde yayımlama

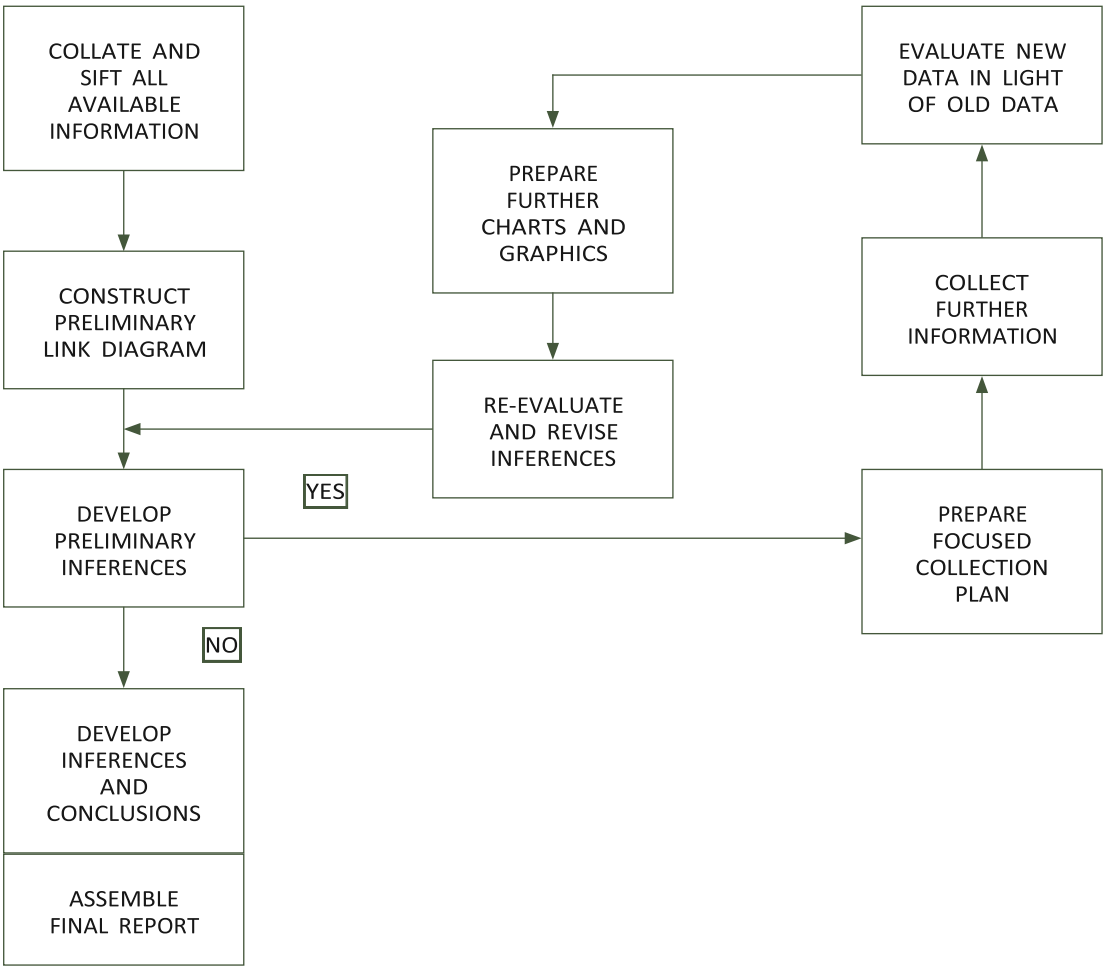
İstihbarat bir analitik ürüne entegre edildiğinde, eğer ürün 'gizli' olarak derecelendirilen herhangi bir istihbarat içeriyorsa, o zaman tüm belgede bu koruyucu işaret olacaktır. Benzer şekilde, herhangi bir ürün 4 işleme koduyla derecelendirildiyse (yalnızca menşe kuruluş içinde dağıtım), o zaman tüm ürün aynı kısıtlamayı taşıyacaktır.

5. Analiz ve analitik süreç

İstihbarat sürecinin analiz aşaması, temel özellikleri vurgulayan mevcut bilgilerin anlamının incelenmesiyle ilgili olduğu için kritiktir.

Analiz, bilgi boşluklarını, güçlü ve zayıf yönleri vurgular ve ileriye giden yolu belirler.

Şekil 5-1. Analitik süreç



Analitik süreç, hem kısa vadeli operasyonel amaçlar hem de uzun vadeli stratejik nedenlerle kanun uygulama hedeflerini yönlendirmek için istihbaratın geliştirilmesi için kritik öneme sahiptir. Analizin kapsamı ve genel güvenilirliği, bilgilerin düzeyine ve doğruluğuna bağlıdır.

analistin becerileri ile birlikte sağlanır. Analiz, her türlü kanun yaptırımı hedefinde gerçekleştirilebilen döngüsel bir süreçtir. Farklı suç türleri ve operasyonlar farklı senaryolar gerektirir, ancak etkili bir analiz yapabilmek için kullanılan bilgi türü yapay önlemlerle değil, bilgilerin mevcudiyeti ve her ülkenin yasal kısıtlamaları ile önceden belirlenmelidir.

Veri entegrasyonu, kolluk kuvvetleri eylemi için çıkarımlar yapmak amacıyla zayıf alanlar oluşturmak için farklı kaynaklardan çeşitli türdeki bilgileri birleştiren analitik sürecin ilk aşamasıdır. Dikkatli entegrasyon, soruşturmadaki bilgi boşluklarını ve zayıflıkları vurgular, böylece analistin, analiz çalışmasının en erken aşamalarında bile veri toplamaya devam etmesini sağlar. Bir soruşturmanın ilk kısmındaki sürecin bu aşaması, analistin sınırlı bilgiye dayalı hipotezler geliştirmeye başlamasına da izin verir.

VERİ ENTEGRASYONU: HAZIRLIKTA VERİLERİN BİRLEŞTİRİLMESİ ÇİZİM ÇİZİMLERİ

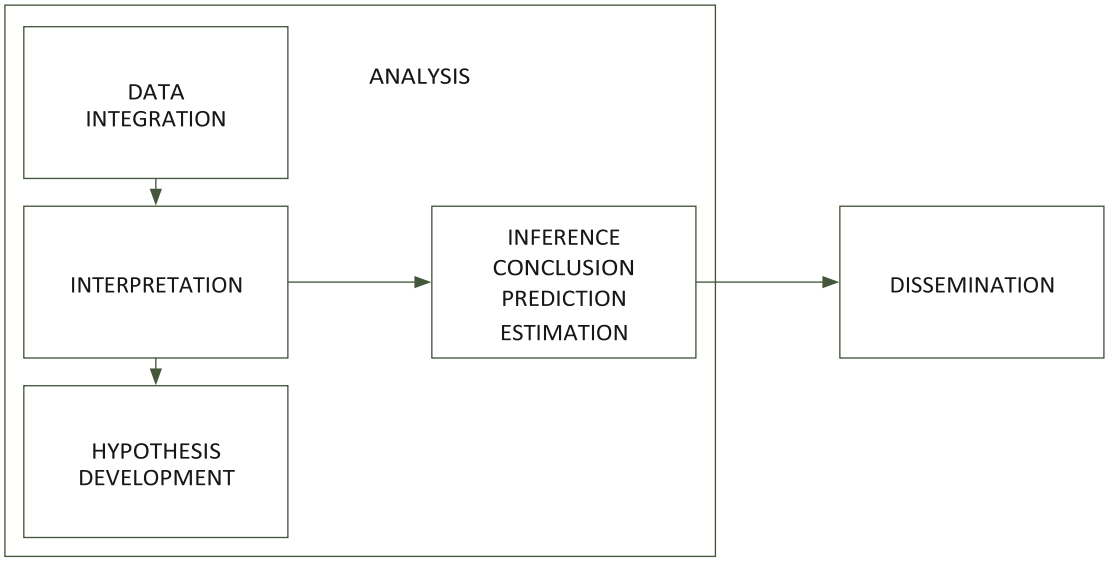
Analitik süreçteki bir sonraki adım, sıklıkla gerçeklerin ötesine geçmek ve "eğer öyleyse" sorularını sormak anlamına gelen yorumlamadır. Bu aşamanın başarılı olması için önceki aşamaların doğru ve

eksiksiz olması, analistin mevcut bilgilere dayanarak bilinçli bir karar verme riskini en aza indirmesi gerekir.

VERİLERİN YORUMLANMASI: VERİLERE ANLAM VERMEK; MEVCUT BİLGİLERİN ÖTESİNE GEÇMEK

Verileri genellikle çizelgeler biçiminde, ancak tablolar veya haritalar olarak da entegre ederek, analist yorumlamanın gerçekleştirilebileceği bir platform yaratıyor. Çizelgeler ve diğer ürünler, brifing yardımcıları veya fikirlerin illüstrasyonları olarak faydalıdır; ancak temel alınan veriler ve anlamı, analizin neyle ilgili olduğudur. Kılavuz, ilk olarak genel istihbarat analizi sürecini anlamaya yardımcı olarak ve ikinci olarak belirli bir sorunun anlaşılmasını belirlemeye yardımcı olarak son derece yararlı oldukları için bu analiz yan ürünlerine odaklanacaktır.

Şekil 5-2. Analiz süreci



Analist, süreci tekrar tekrar takip ederek, halihazırda geliştirilmiş olan hipotezleri desteklemeye veya çürütmeye başlayabilir. Orijinal bir fikrin yanlış olup olmaması önemli değildir, en önemli husus onun yanlış olduğunu tespit etmektir. Genel sorgulama devam ettikçe, fikirlerin doğruluk derecesi daha da güçlenir ve analist daha sonra hipotezlere daha fazla güvenmeye başlayabilir.

Böylece bir hipotez, daha fazla veri toplamaya odaklanabilecek bir teori sağlar. Hipotez veya herhangi bir çıkarım şunları içermelidir:

Önemli birey veya bireyler	- KİM?
Suç faaliyetleri	- NE?
Çalışma yöntemi	- NASIL?
Coğrafi kapsam	- NEREDE?
Motif	- NEDEN?
Zaman çerçevesi	- NE ZAMAN?

Yapılan hipotezler veya çıkarımlar operasyonel ekipler tarafından test edilebilir ve bu durumda geri bildirim esastır. Hipotezler çok fazla spekülasyon içerir ve araştırmadan çıkan bulgularla doğrulanması, değiştirilmesi veya reddedilmesi gerekir. Hipotezleri test etmek için yapılandırılmış veri toplama esastır ve bu nedenle bir toplama planı geliştirilmelidir.

Analiz sürecinde, analistler için aşağıdaki aksiyomlar ve standartlar dikkate alınmalıdır.

BİR ISTIHBARAT ANALİSTİ İÇİN GERÇEKLER

Kendi mesleki yargınıza inanın

Uzman sensin. İşinize inanın ve istihbaratnız pozisyonunuzu destekliyorsa yerinizi alın.

Risk alan biri olun

Trendleri veya olayları tahmin ederken yanılmaktan korkmayın. Risk almak, iş tanımınızın bir parçasıdır. Yalnızca risk alarak ajansınıza olan değerinizi en üst düzeye çıkarabilirsiniz.

Hiç bir şey yapmamaktansa hata yapmak daha iyidir

Eğer yanılıyorsan ve gerçekler bunu gerektiriyorsa, kabul et. Sadece hiçbir şey yapmayanlar hata yapmaz.

Her ne pahasına olursa olsun ayna görüntülemeden kaçının

Ayna görüntüleme, düşünce sürecinizi veya değer sisteminizi başka birine yansıtmaktır. Hedefleriniz suçlular. Onların zihniyeti tamamen farklı. Onlar gibi düşünmeyi öğrenmelisin.

Yayılmadıkça istihbaratın hiçbir değeri yoktur.

İstihbaratı, sonuçları ve tavsiyeleri açık, etkili ve zamanında iletin. Müşterinizin bilmediği şeyin değeri yoktur.

Herkes bir konuda hemfikir olduğunda, muhtemelen bir şeyler yanlıştır.

İstihbarat camiasındaki bir grup insanın herhangi bir konuda tam olarak hemfikir olması nadirdir ve doğal değildir. Eğer gerçekleşirse, endişelenmenin zamanı geldi.

Müşteriniz ne kadar bildiğinizi umursamıyor, onlara sadece bilmeleri gerekenleri söyleyin

Aşırı ayrıntılar sadece önemli gerçekleri gizler.

Biçim hiçbir zaman maddeden daha önemli değildir

Profesyonel bir görünüm ve uygun şekilde seçilmiş formatlar önemlidir, ancak özden daha ağır basmazlar. Müşteriler istihbaratnın ne anlama geldiğini bilmek isterler ve ihtiyaç duyduklarında onu isterler.

İhtiyacınız olan bilgi toplamayı agresif bir şekilde takip edin

Asla ihtiyacınız olandan daha azına razı olmayın. Herhangi bir nedenle hayati veri kaynağına erişemezseniz, sorumlu tutulacaksınız.

Düzenleme sürecini kişisel algılamayın

Editöryel değişiklikler mesajınızın anlamını değiştirmiyorsa, kabul edin. Eğer yaparlarsa, konuşun. O zaman bile, daha parlak bir zihin sizin neyi kaçırdığınızı görmüş olabilir. Ürününüze inanın, ancak öz eleştiri yapın.

İstihbarat topluluğu meslektaşlarınızı tanıyın ve onlarla konuşun

Siz rakip değilsiniz; aynı cinssiniz. Ağın bir parçası olun. Telefonu yalnızca bir şeye ihtiyacınız olduğunda açmayın.

İşinizi veya kendinizi çok ciddiye almayın

Tükenmişlikten kaçının. Sizi bir varlık olarak silmek, ajansınız için net bir kayıp olacaktır (ancak hemen tam olarak böyle görmeyebilir). Ailenizin ve sağlığınızın refahı, bir suçluyu alt etmek veya kariyer basamaklarında bir basamak daha yükselmekten daha önemlidir. Daha büyük düzendeki rolünüz kendi kendine önemli değildir. İşe olan bağlılığınız, azim ve bağlılığınız ancak uzun vadede sonuç getirecektir.

ANALİSTLER İÇİN ON STANDART

1. Analiz edilen veriler (yani istihbarat), kolluk kuvvetleri operasyonlarını ve soruşturmalarını yönlendirmek için kullanılmalıdır.

2. Analiz, ajansın takip ettiği her büyük soruşturmanın ayrılmaz bir parçası olmalıdır.

3. Analitik ürünler, asgari olarak yazılı bir rapor içermelidir. Görsel ürünler de sunulabilir, ancak bunlar yalnızca yazılı bir raporun yerine geçmek yerine ona ek olarak kabul edilebilir.

4. Analitik ürünler sonuç ve tavsiyeler içermelidir. Bunlar, karar alma süreçlerine ilişkin değerlendirmeleri için yönetime sunulur.

5. Analitik bir ürünün geliştirilmesi, düşüncenin verilere uygulanmasını gerektirir. Karşılaştırma veya diğer hususları yansıtmayan veri derlemesi, analiz değildir.

6. Analitik ürünler doğru olmalıdır. Tüketiciler, analistler tarafından kendilerine sağlanan verilere güvenebilmelidir.

7. Analizler zamanında yapılmalıdır.

8. Analitik ürünler, analist için mevcut olan kaynaklar ve araçlar aracılığıyla mevcut tüm ilgili verileri yansıtmalıdır.

9. Analizler, analistin ortamında mevcut olan en iyi ve en güncel bilgisayar programlarını, derlemeyi, görselleştirmeyi ve analitik teknikleri içermelidir.

10. Analizler, üretildikleri kurum veya kuruluşun misyonuna ve önceliklerine niteliksel ve niceliksel katkılarını hem yansıtmalı hem de bunlara göre değerlendirilmelidir.

6. Temel analiz teknikleri: bağlantı analizi

GİRİİŞ

Bir araştırmadaki pek çok ham veri, karmaşık ve ayrıntılı yazılı raporlar halinde harmanlanır. Suç girişiminin veya şüpheli suç faaliyetinin analizine ilişkin diğer veriler genellikle çok hacimlidir ve çeşitli biçimlerdedir.

İstihbarat analistleri için temel sorun, bilgiyi organize bir şekilde bir araya getirmektir, böylece bir araya getirilen bilgiden anlam çıkarmanın zor görevi daha kolay hale getirilir.

Bağlantı analizi, varlıklar (bireyler, organizasyonlar, yerler vb.) arasındaki ilişkiler hakkındaki bilgileri, ilişkileri netleştirecek ve çıkarım geliştirmeye yardımcı olacak bir grafik formatına ve bağlama yerleştirir. Bağlantı analizi, belirli bir analizde tanımlanmış olabilecek bu varlıklar arasındaki ilişkilere uygulanabilir.

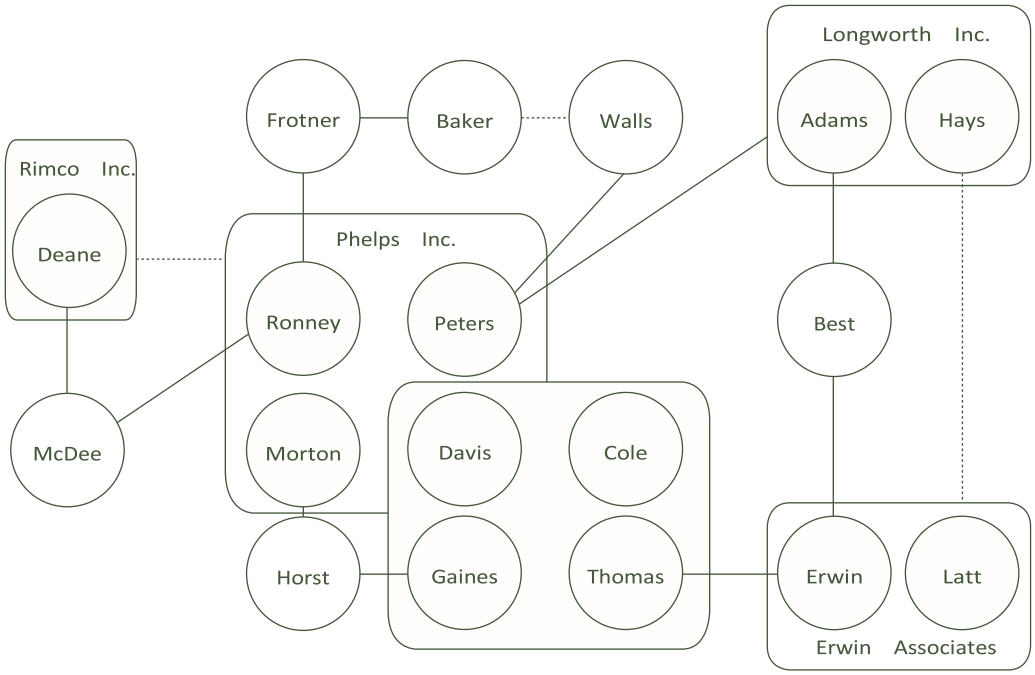
Bağlantı analizi yedi adımlı bir süreçtir. Sürecin ürünü, şekil 6-1'de gösterilen örnek gibi bir bağlantı şemasıdır.

Bağlantı analizinin yedi adımı şunlardır:

1. Tüm ham verileri birleştirin
2. Grafiğin odağını belirleyin
3. Bir ilişki matrisi oluşturun
4. İlişkileri matriste kodlayın
5. Her varlık için bağlantı sayısını belirleyin
6. Bir ön çizelge çizin
7. Grafiği netleştirin ve yeniden çizin

Lütfen aşağıdaki ayrıntılı metodolojinin manuel yollarla bağlantı analizi uygulamasını açıkladığını unutmayın. Bilgisayar uygulamalarının kullanılması, bu sürecin mekaniğini büyük ölçüde basitleştirir, ancak yine de aynı analitik düşünce sürecinin izlenmesini gerektirir.

Şekil 6-1. Örnek bağlantı şeması



1. Tüm ham verileri birleştirin

İlgili tüm dosyaları, saha raporlarını, muhbir raporlarını, kayıtları vb. bir araya getirin.

2. Grafiğin odağını belirleyin

Grafiğinizin odak noktası olacak varlıkları belirleyin. Verilerinizi okuyun ve kişilerin ve/veya Kuruluşların adlarını, otomatik lisans numaralarını, adresleri vb. içerebilecek bu varlıkların altını çizin veya vurgulayın.

3. Bir ilişkilendirme matrisi oluşturun

Bir ilişki matrisi (şekil 6-2), bir bağlantı şeması oluşturmanın temel, geçici bir adımıdır. Varlıklar arasındaki ilişkileri tanımlamak için kullanılır, ancak sunum amacıyla kullanılmaz. Hangi çizelgelerin oluşturulacağına bakılmaksızın, her zaman önce bir ilişki matrisi oluşturulmalıdır.

Şekil 6-2. Örnek ilişkilendirme matrisi

Derneğin temeli şehirler arası mesafedir.

Londra ve Rio de Janeiro arasındaki mesafe, Londra sütunu ile Rio de Janeiro satırının kesiştiği noktada bulunabilir, bu durumda bu 5.750 mil gösterir. Bu iki şehir arasındaki ilişki

Matrisin köşegen eksenine grafik yapımına konu olan varlık isimleri girilir.

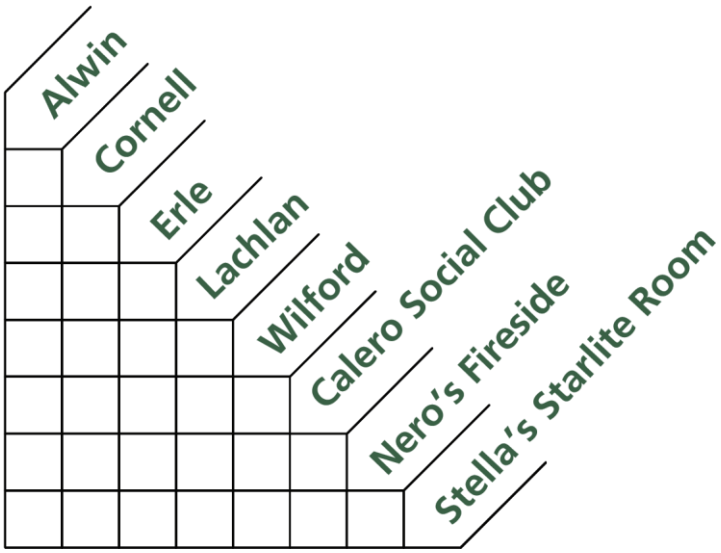
Kişiler alfabetik sıraya göre listelenmelidir.

Kuruluşlar, kişilerden sonra alfabetik sıraya göre listelenmelidir.

Araç Tescil İşaretleri veya adresleri vb. kullanılan varlıklar olduğunda, organizasyonlardan sonra alfanumerik olarak düzenlenmelidir. Bu eylem, matrisi kontrol ederken yardımcı olacaktır.

Kuruluş adından önce bir yıldız işareti (*) eklenmesi, çağrışımların sayılmasını kolaylaştırabilir.

Şekil 6-3. Kişi ve kuruluşların isimlerini kullanan ilişkilendirme matrisi



Şekil 6-3'te gösterilen matris için, ilişkinin temeli, bireyler, bir birey ve bir organizasyon veya organizasyonlar arasında doğrulanmış veya olası bir bağlantının kanıtı olacaktır.

4. Çağrışımları matriste kodlayın

İlişki kodları, matriste gösterilen her ilişkinin temelini veya yapısını belirtmek için kullanılır. Önerilen ilişkilendirme kodları ve olası anlamları şekil 6-4'te gösterilmiştir.

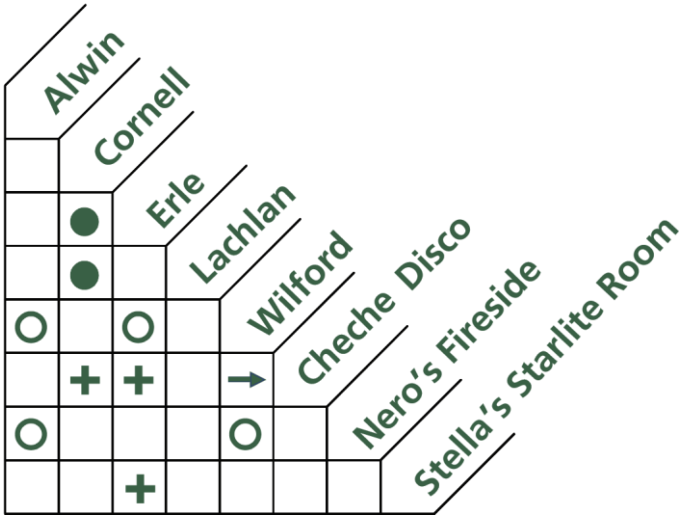
Şekil 6-4. Önerilen ilişkilendirme kodları

ilişki kodları	
kod	**Anlam**
●	İki varlık arasında doğrulanmış ilişki
O	İki kuruluş arasında şüpheli ilişki
+	Kuruluşun onaylanmış üyesi—memur, yönetici, çalışan, kulüp üyesi
-	Örgüte şüpheli üyelik
➔	Başka bir katılım olmadan onaylanmış yatırım - hissedar, limited ortak (sahipten sahipliğe yön)
▶	Başka bir katılımı olmayan şüpheli yatırım (sahibinden sahip olunan yöne)

Onaylanmış bağlantılar, bilgilerin A1, A2, B1 veya B2 olarak değerlendirildiği yerlerdir.

Onaylanmamış bağlantılar, bilgilerin başka bir şekilde değerlendirildiği yerlerdir.

Şekil 6-5. Tamamlanmış ilişkilendirme matrisi



Girişler şu şekilde yorumlanır:

Erle , doğrulanmış bir birliktelik

Cornell ve Lachlan, doğrulanmış bir birliktelik

Alwin ve Wilford, doğrulanmamış bir birliktelik

" Erle ve Wilford, doğrulanmamış bir birliktelik

" Alwin, Nero'nun Fireside ile doğrulanmamış bir ilişki

Cornell, Cheche Disco'ya onaylanmış bir katılımcı

" Erle, Cheche Disco'ya onaylanmış bir katılımcı

" Wilford, Nero'nun Fireside ile doğrulanmamış bir ilişki

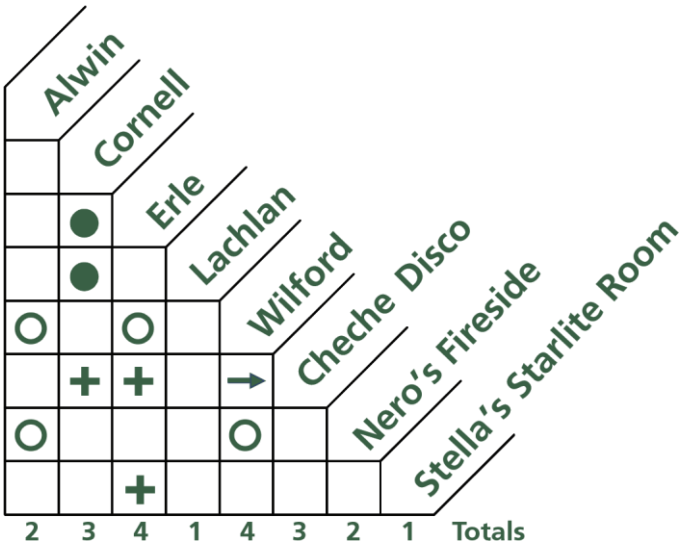
" Erle, Stella'nın Starlite Odasında onaylanmış bir katılımcı

Wilford, Cheche Disco'da bir memur değil, hissedar olduğunu doğruladı

5. Her varlık için bağlantı sayısını belirleyin

Grafiğinizi başlatmanın yararlı bir yolu, matristeki her bir varlıkla ilişkili bağlantıların sayısını saymaktır. Her varlık için baştan ve aşağı saydığınızdan emin olun. Şekil 6-6 prosedürü göstermektedir.

Şekil 6-6. Her varlık için bağlantıların toplamı



6. Bir ön çizelge çizin

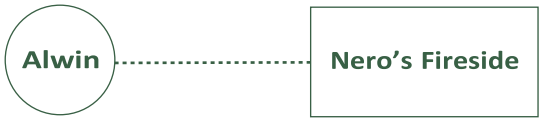
İlişkilendirme matrisinde yer alan tüm bilgileri grafiksel olarak gösteren bir çizelge çizin. Bu, ilgili sembolleri seçip kullanarak yapılabilir. Şekil 6-7 ve 8-8'de gösterilen başlangıç çizelgeleri, bireyleri temsil etmek için daireler ve organizasyonları temsil etmek için dikdörtgenleri kullanır.

Şekil 6-7. Onaylanmış bağlantı

Onaylanan bağlantılar düz çizgilerle ve şüpheli bağlantılar noktalı çizgilerle gösterilir. Sahiplik, düz bir çizgi üzerinde yüzde etiketi ile belirtilebilir.

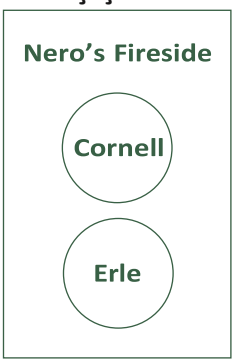
Cornell ve Lachlan arasında bilgiye dayalı olarak onaylanmış bir bağlantı var.

Şekil 6-8. Onaylanmamış bağlantı



Alwin ve Nero'nun Fireside'ı arasında bilgiye dayalı olarak doğrulanmamış bir bağlantı var.

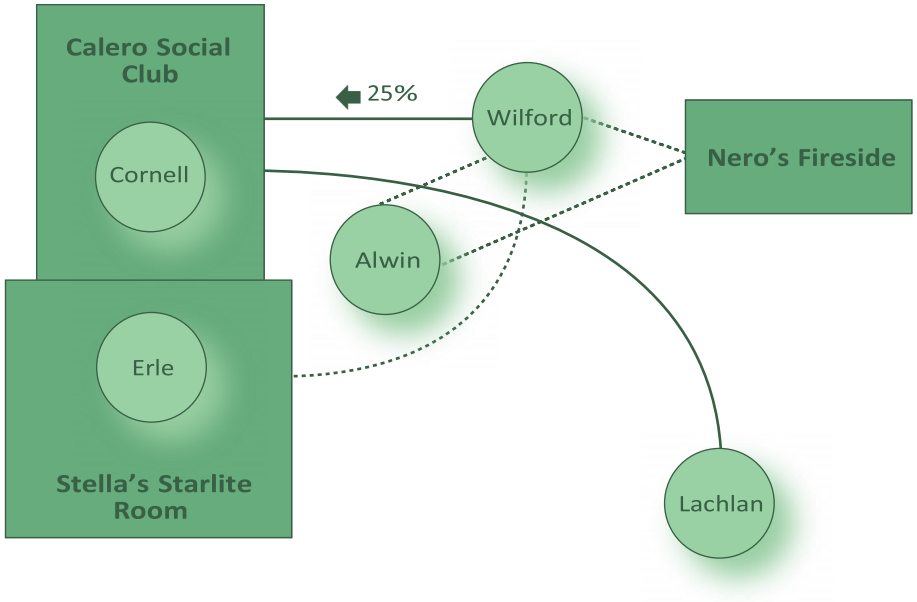
Şekil 6-9. Bir kuruluş içindeki varlıklar



Cornell ve Erle, Calero Social Club örneğinin organizasyonuyla ilgilenmektedir: Sekreter ve Yönetici.

Kuruluş içindeki rolleri nedeniyle iki kişi arasında zımni bir bağlantı olabilir. İkisi arasında düz bir çizgi, aralarında kesin bir ilişki olduğunu gösterir. Şekil 6-9'da gösterilen örnekte, bağlantıyı destekleyecek herhangi bir bilgi bulunmamaktadır. Ancak, analizinize dayanarak, varsayımsal bir bağlantı hattı göstermek için bir neden olduğunu hissedebilirsiniz.

Figure 6-10. Preliminary link chart



7. Grafiği netleştirin ve yeniden çizin

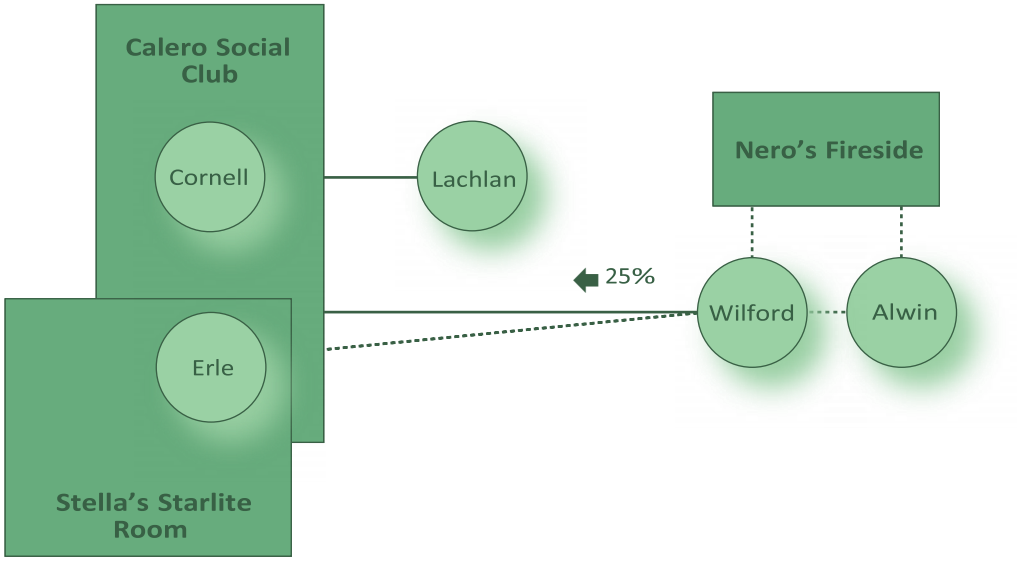
Varlık sembollerini yerleştirirken ortaya çıkan uzun ve/veya çapraz çizgiler, gösterilen ilişkileri karıştırabilir veya yorumlamayı zorlaştırabilir. Grafiğin yeniden çizilmesi, varlıklar arasındaki ilişkileri netleştirmeye yardımcı olabilir.

Bu adımın tamamlanması, arka sayfada gösterilen nihai çizelgeyle sonuçlandı. Tüm çizelgeler zamanlanmış, tarihli ve sıra numaralı olmalıdır. Bu, daha eski ve daha yeni çizelgeler arasında ayrım yapılmasına yardımcı olacak ve çizelgenin ne zaman oluşturulduğunu izleyiciye gösterecektir - özellikle ifşa sorunlarıyla ilgili bir faktör.

Grafiğe bir anahtar eklenmelidir.

Bu adımın tamamlanması, şekil 6-11'de gösterildiği gibi nihai tabloyla sonuçlandı.

Şekil 6-11. Şekil 6-10'un yeniden çizilen tablosu



ÇİZELGELERİN DÜZENİ

Grafik düzeni, bir analistin hayal gücü ile geliştirilebilir ve bu nedenle biçim olarak önemli ölçüde değişebilir.

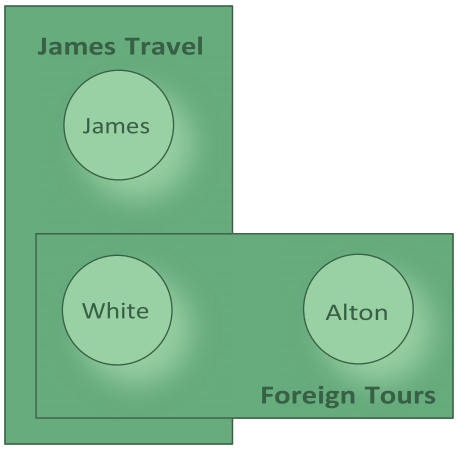
Ancak temel ilke, çizelgelerin bilgiyi basitleştirmesi, yani "resim bin kelimeyi boyar" olmasıdır. Bu nedenle çizelge açık, karmaşık, düzenli ve özlü olmalıdır. Bir dizi fikir mevcuttur ve yalnızca deneyim, bir grafiğin tüm bu kriterleri karşılayıp karşılamadığını gösterecektir.

Her zaman bugün oluşturduğunuz çizelge yarın tamamlanan çizelge kadar iyi olmayacaktır.

GRAFİK DÜZENİ ÖRNEKLERİ

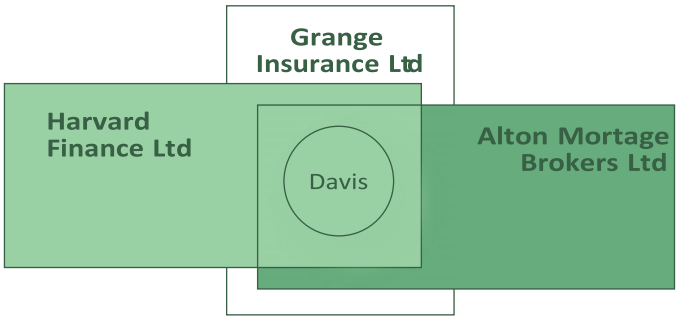
Her birinde başka bir yetkili bulunan iki şirkette yer alan bir kişi:

Şekil 6-12. Düzen örneği 1



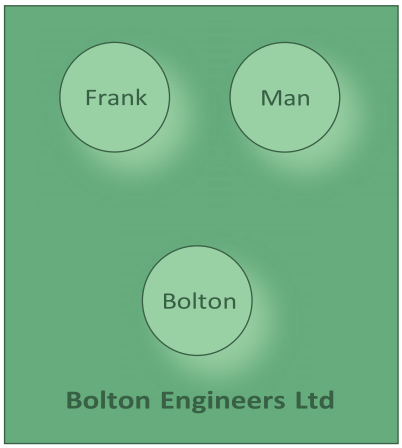
Üç şirkete dahil olan bir kişi, dahil olan başka bir yetkili:

Şekil 6-13. Düzen örneği 2



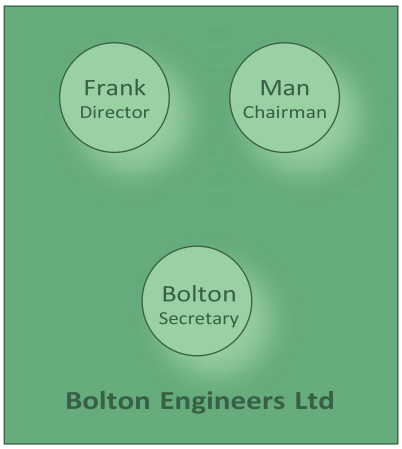
Bağlantıları gösterilen bir şirkette üç kişi (resmi pozisyon gösterilmemiştir):

Şekil 6-14. Düzen örneği 3



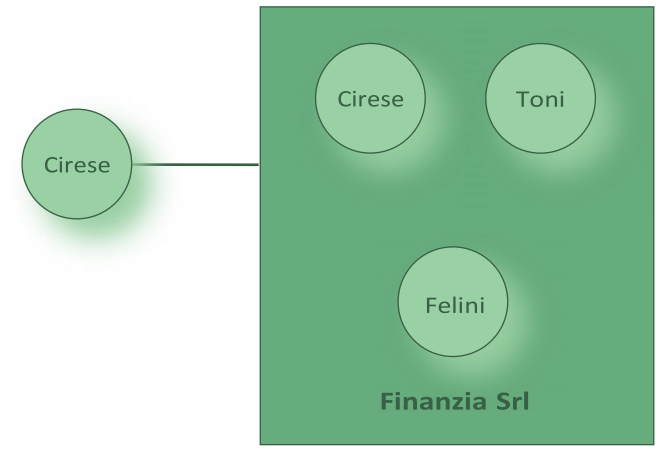
Aynı şirkete dahil olan üç kişi, bağlantılar çıkarıldı ve gösterilen resmi pozisyon:

Şekil 6-15. Düzen örneği 4



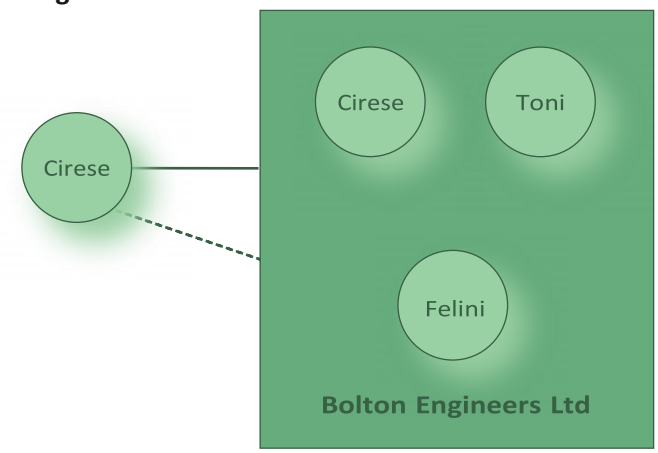
Bir şirkete bağlı olan ancak şirketin yetkilisi olarak gösterilen kişilere bağlı olmayan kişi:

Şekil 6-16. Düzen örneği 5



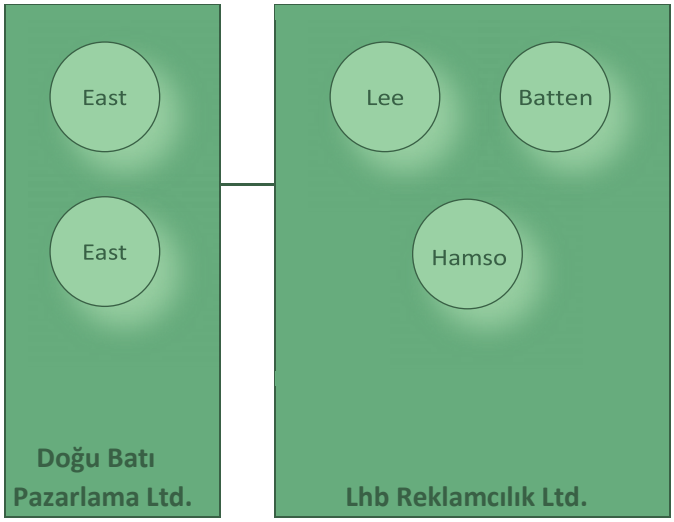
Şirket dışından ancak şirketle bağlantısı olan ve şirket yetkilisiyle bağlantısı olduğundan şüphelenilen kişi:

Şekil 6-17. Düzen örneği 6



İki şirket arasındaki ilişki, ancak şirketlerin bireysel yetkilileri arasında bilinen bir bağlantı yok:

Şekil 6-18. Düzen örneği 7

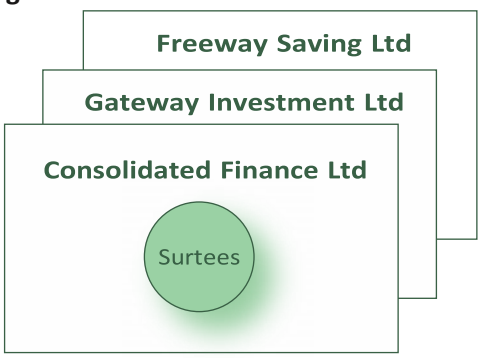


Bilinmeyen bir kişiyle ilişkili bir kişi:

Şekil 6-19. Düzen örneği 8

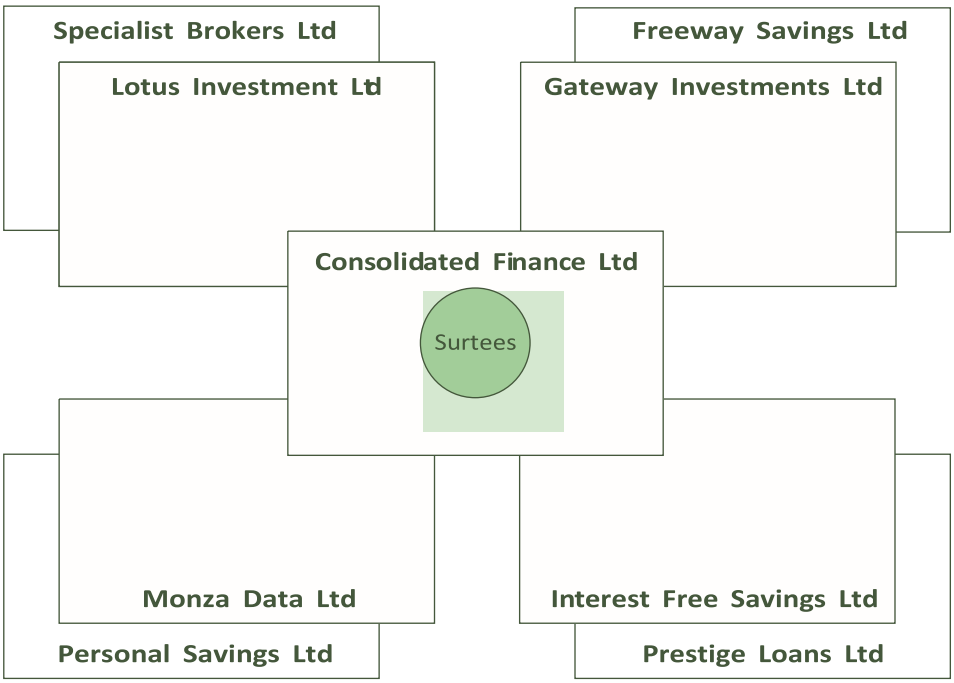
Birbirinin yan kuruluşu olan bir dizi şirketin yetkilisi olan bir kişi:

Şekil 6-20. Düzen örneği 9



Birçok yan şirketi olan bir şirket:

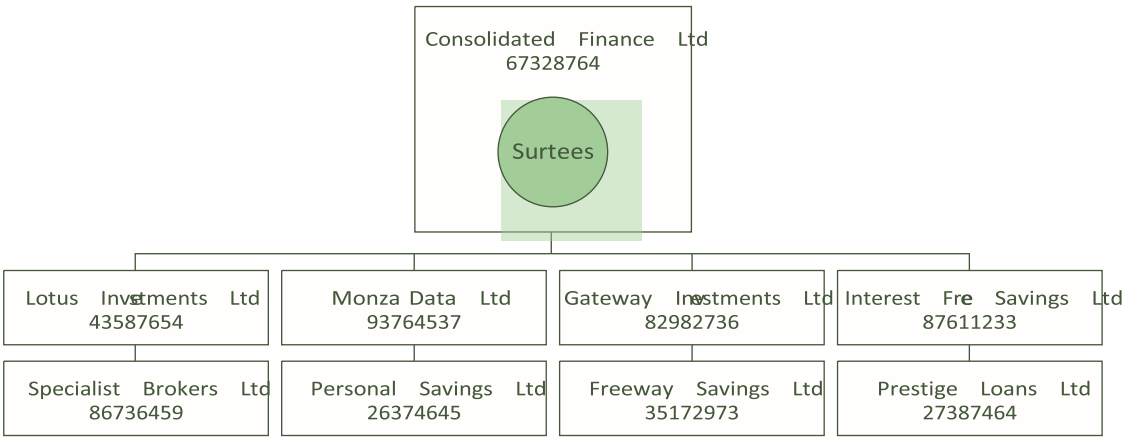
Şekil 6-21. Düzen örneği 10



Bu tür bir çizelge, bir soy ağacıyla aynı şekilde gösterilebilir. Oldukça sık olarak şirketler hakkında bilgi arandığında, Dun & Bradstreet Worldbase gibi ticari veri tabanlarında ana şirket ve nihai sahip hakkında bir gösterge vardır. Diğer bağlantılı şirketleri bulmak için şirket isimleri ve referans numaraları ve yönetici isimleri aranabilir. Mali soruşturmalarda bunlar özellikle yararlıdır.

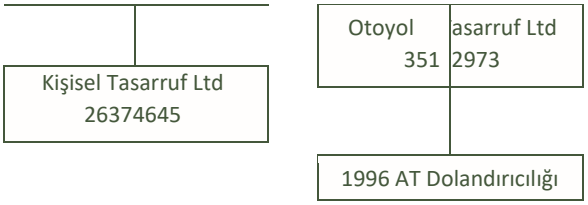
Bu tür bilgilerin grafikli bir örneği aşağıdaki gibidir:

Şekil 6-22. Düzen örneği 11



Gerekirse, her bir şirketin sahiplik yüzdesine ilişkin ayrıntılar, tabloyu daha net hale getirmek için bağlantıya eklenebilir.

Buna ek olarak, şirketin herhangi bir suç faaliyetine karışması da genel tablo hakkında daha fazla bilgi vermek için çizelgede gösterilebilir.



Bir bağlantı şeması oluşturmak, ilişkilendirme analizinin bir ön koşulundan başka bir şey değildir. Bir çizelge kendi başına analitik bir ürün değil, analitik bir araçtır. Bağlantı analizi sadece bağlantılara bakmamalı, aynı zamanda ilişkilerin güçlü yönlerine ve alaka düzeyine de bakmalıdır.

BİR AĞIN ÖNEMLİ ÖZELLİKLERİ İÇERİR
DÖRT KAVRAMDA: VARLIK, İLİŞKİ, YÖNLÜLÜK, GÜÇ

Varlıklar , insanları, işletmeleri, organizasyonları, ulaşım araçlarını, yerleri, olayları, nesneleri vb. içerebilecek inceleme altındaki öğelerdir .

İlişkiler ailevi olabilir veya karşılıklılık (değişim ve uzlaşma), uygunluk (işi yapacak doğru kişi), bağ (geçmiş dernekler), kontrol (cezai hiyerarşi veya tehdit), baskınlık, üstünlük, tabi olma gibi alma ve verme temelli olabilir. ve ardıllık.

Yönlülük , bilgi akışı, *iyilik* ve yetki ile ilgilidir ve bir ağın iç mekaniğinin anlaşılmasını sağlar.

" *Güç* , ilişkilerde yer alan etkileşimlere ve sağlanan verilerin değerlendirilmesine dayanan öznel bir yargıdır.

Bir süreç olarak ilişki analizi, zengin bir veri tabanından çeşitli bağlantılar hakkında bilgi içerecektir.

Bir çizelge, kuruluş veya ağın üyeleri arasındaki derneklerin durumuna ilişkin hipotezlerin toplanabileceği çalışan bir üründür. Düşünen bir ilişkilendirme analizinin özellikleri, ilişkilere ve bağlantılara, bunların güçlü yönlerine ve amaçlarına, bu bağlantıların kuruluş ve bir kuruluşu araştıranlar için ne anlama geldiğine bakmayı içerir.

Genellikle bir ilişkilendirme grafiği, grubun yalnızca "kareyi dondur" anlık görüntüsünü gösterir. Grubun zaman içindeki gelişimini göstermek daha uygun olabilir.

İlişkilendirme analizinde bağlantı sorunları

1. Bu organizasyonun merkezinde kim var?
2. Veritabanındaki hangi isimler takma ad olarak görünüyor?
3. Hangi üç kişinin bir tedarik ağını kesmesi veya devre dışı bırakması?
4. Belirli bir kişi bir suç örgütü içinde hangi rolleri oynuyor gibi görünüyor?

5. En çok hangi iletişim bağlantıları izlenmeye değer?
6. Hangi etkileşim kalıpları görülebilir ve bu kalıplar davranışı anlamamıza ve tahmin etmemize nasıl izin verir?
7. Gruptaki bireyler arasında değiş tokuş edilen bilgilerin doğası nedir?
8. Üyelerinin faaliyetlerini hangi grup baskıları veya yazılı olmayan kurallar yönetir?
9. Etkileşimler ne sıklıkla?
10. Etkileşimlerin başlatıcısı kimdir?
11. Farklı kuruluşlar arasında kim bir köprü veya irtibat kurar?
12. Kaldırılırlarsa kilit kişiliklerin rollerini üstlenebilecek kişiler kimlerdir?
13. Kuruluşun finansal bağlantıları, faaliyetleri hakkında bize ne söylüyor?
14. Hangi iş bağlantıları var?
15. Diğer suç faaliyetleriyle ne gibi bağlantıları var?
16. Coğrafi konumlara, 'bölgeye' bağlantılar nelerdir?
17. Örgütün hiyerarşisi nedir?
18. Suç faaliyeti nasıl organize edilir?
19. Grup organizasyonu onu sızmaya karşı savunmasız hale getiriyor mu?
20. Örgüt, haraç alma veya devam eden suç teşebbüsü tüzükleri kapsamında kovuşturulabilir mi?
21. Linkler zamanla değişti mi?
22. Daha önce hangi bağ elementleri biliniyordu?
23. Bağlantıların gücü veya merkeziliği değişiyor mu?
24. Bazı üyeler, diğer üyeler hariç tutulacak şekilde diğer bazı üyelere bağlı mı?
25. Örgüte üyelik için kriterler var mı?
26. Kuruluşun şiddet kullanımına yönelik eğilimi nedir?
27. Suç grubu ile düzenleyici veya hükümet yapısı arasında herhangi bir bağlantı var mı?
28. Grup liderinin yönetim felsefesi hakkında ne bilinir?
29. Bu bağlantı modeli diğer suç örgütlerine uygulanabilir mi?
30. Bu veya diğer yargı alanlarında daha önce benzer yapılara sahip başka gruplar oldu mu?
31. Bu grubun yapısı, gelecekteki benzer suç gruplarının yapısını tahmin etmemizi sağlıyor mu?

İlişki Analizi Format Modeli

Bu, aşağıdakilerden oluşmalıdır:

- Analiz bulgularının yönetici özeti.
- Önceki bağlantı sorunları listesinden ilgili soruların yanıtlarıyla birlikte gruba genel bir bakış.
- Grubu betimleyen bir bağlantı grafiği veya bir dizi grafik.
- Her bir araştırma hedefi ve potansiyel hedef hakkında biyografik özetler.
- Grup hakkında sonuçlar.
- Yanıtlanacak soruların bir listesi de dahil olmak üzere daha fazla taktik veya stratejik eylem için öneriler
- ve olası bilgi kaynakları (istihbarat açıklarını vurgulayın).

İlişkilendirme analizine Süreç Odaklı Yaklaşım uygulanarak, bu bölümün başında açıklanan standart yedi adımlı süreç aşağıdaki şekilde genişletilebilir:

1. Veri topla
2. Verileri düzenleyin/düzenleyin
3. İlişkilendirme materyalini çıkar
4. İlişkilendirme matrisi hazırlayın
5. Bağlantı grafiğini hazırla
6. Grafikteki varlıkların biyografik özetlerini üretin
7. Grafiği özetle
8. Soruları/sorunları kuruluşa veya ağa uygun şekilde uygulayın
9. Hangi gerekli bilgilerin mevcut olduğunu ve neyin bulunmadığını belirleyin
10. Ara hipotez(ler)i çizin
11. Bu bilgilerin toplanması ve atılacak daha ileri soruşturma veya kovuşturma adımları için cevaplanmamış soruların ve tavsiyelerin bir listesini geliştirin.
12. Bulguları ve yazılı bir raporu yönetime sunmak

7. Temel analiz teknikleri: olay grafiği

Bir olay çizelgesi, ilgili bir dizi olaydan anlam geliştirmek için uygun bir araçtır. Bir olay çizelgesi, meydana gelme zamanları ve olaylar arasındaki ilişkiler netleşecek şekilde bir olaylar dizisini gösterir. Olay çizelgesi, karmaşık bir vakanın analizinin başlarında geliştirilmelidir. Olay grafiği aşağıdaki bileşenlerden oluşur:

" Olayların kısa açıklamaları, daire veya dikdörtgen gibi sembollerde bulunur. Herhangi bir grafikte, bir sembolün her kullanıldığında aynı şeyi temsil ettiğinden emin olun. Olayların açıklamalarını kısa tutun - üç veya dört kelimeden uzun değil.

" Bağlantı çizgileri, olaylar arasındaki ilişkileri belirtmek için kullanılır - bir olayın diğerine yol açtığı olayların zaman dizisi.

" Her satırdaki bir ok, olayların sırasını - olayların zaman içindeki akışını gösterir.

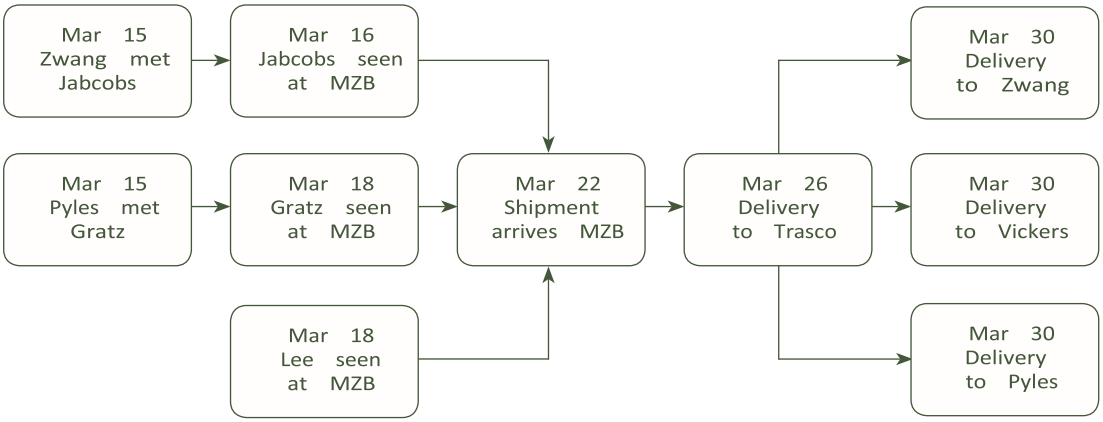
" Her bir olayla ilişkili tarih ve/veya saat, bir şekilde olayın açıklamasına bağlıdır - olay sembolü içinde, sembole yakın veya sembolle bağlantılı.

Olaylar genellikle sırayla raporlanmadığından, tarih ve saatleri dikkatli bir şekilde not edin. Bu bileşenler, yalnızca analizin amacı ve analistin yaratıcılığı ile sınırlı olmak üzere, çeşitli şekillerde bir olay çizelgesinde birleştirilebilir. Bir olay çizelgesinin oluşturulmasındaki ana faktörler, *(a)* bilgilerin açık ve doğru bir sunumunu sağlamak ve *(b)* çizelgeyi mümkün olduğunca basit ve noktaya kadar tutmaktır.

Nihai çizelge, analistin bir suç faaliyetindeki olayların önemini görselleştirmesi için güçlü bir araçtır. Bu görselleştirmeyi azaltabilecek hiçbir şey grafikte yer almamalıdır.

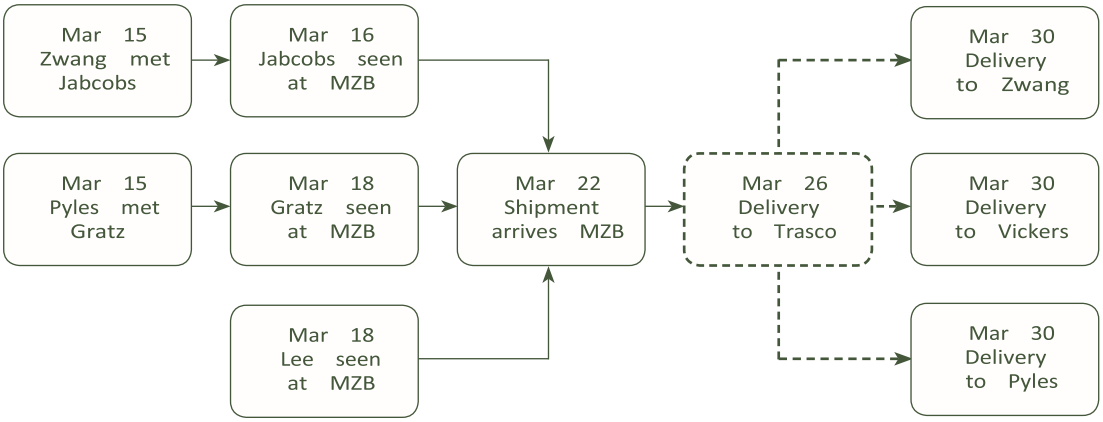
En sık kullanılan olay grafiği türü, şekil 7-1'de gösterilendir. Bu çizelgede, bağlantı çizgileri ve oklar dışındaki tüm bilgiler olay sembolü (olayın tarihi ve açıklaması) içinde yer almaktadır.

Şekil 7-1. Bir olay şeması örneği



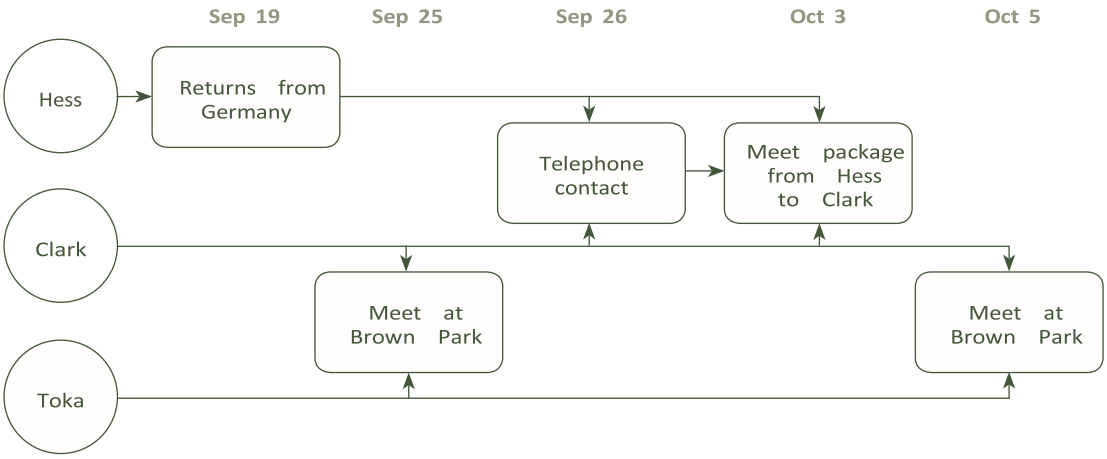
Bir olay grafiği hem doğrulanmış hem de varsayımsal bilgileri gösterebilir. Örneğin, başka koşullar altında, 26 Mart'ta Trasco'ya bir teslimat yapıldığından şüphelenebiliriz. Ancak, henüz böyle olduğunu teyit etmedik. Varsayımsal bir olay, şekil 7-2'deki çizelgede gösterilmektedir.

Şekil 7-2. Varsayımsal bir olay içeren bir olay grafiği örneği



Birkaç varlığı (bireyler veya kuruluşlar) çevreleyen olayların modelini ortaya çıkarmak önemliyse, bir olay matrisi grafiği daha uygun olabilir. Bir olay matrisi grafiği örneği, şekil 7-3'te gösterilmektedir.

Şekil 7-3. Olay matrisi grafiği örneği



Matris terimi, grafikte (şekil 7-3) matrisin bir tarafındaki (örnekte sol taraftaki) bireyleri ve diğer taraftaki (örnekte en üstteki) zamanı listelediği için kullanılmıştır. Bu formatta, önemli olaylar, zaman ve bireyler

arasındaki kesişme noktalarında çizilir. Oklar bir bireyden sadece o bireyin dahil olduğu olaylara gider. Bir olayda birden fazla kişi yer alıyorsa, kişinin satırları arasında sembolü gösterin.

Genel olarak olay matrisi çizelgelerinde, yatay ölçek zamandır ve dikey olan, kişiler, telefonlar, araçlar vb. veya bu tür varlıkların herhangi bir kombinasyonu olabilen temalara bölünmüştür. Olay matrisi çizelgeleri son derece büyük ve karmaşık olabilir ve en iyi şekilde ısmarlama bilgisayar yazılım paketleri kullanılarak oluşturulur.

8. Temel analiz teknikleri: akış analizi

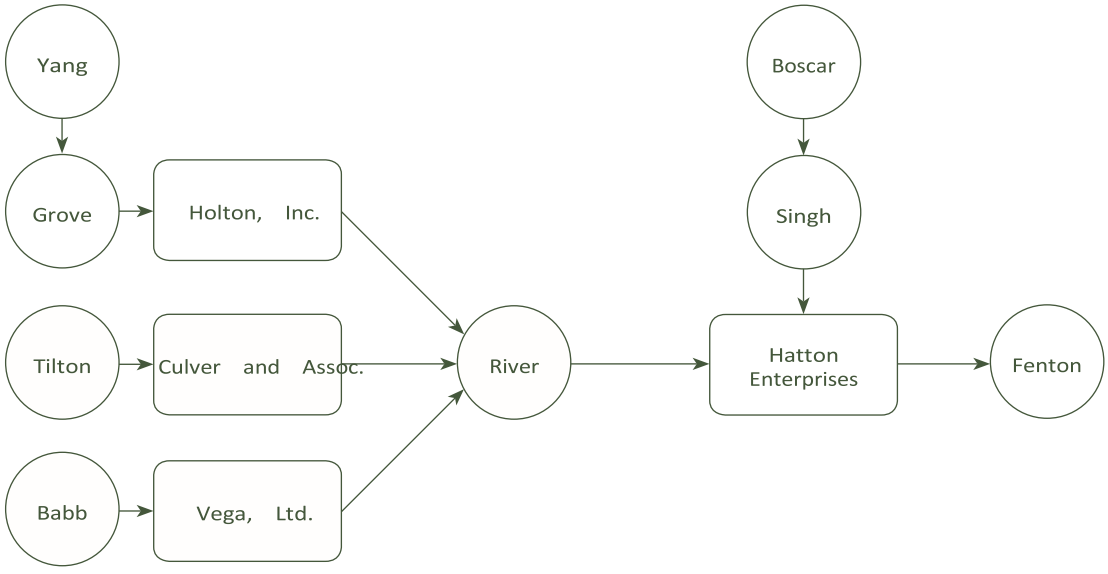
Suç örgütlerinin çoğu, zenginlik yaratmak için para, uyuşturucu ve mal gibi bir tür meta elde etmek için faaliyetlerini yürütür.

Tüm bu malların bir kuruluştan akması gerekir ve bu akış anlaşılırsa, kuruluşun nasıl çalıştığına dair bilgi edinilebilir, böylece daha verimli kolluk eylemi yapılabilir. Örneğin, bir kuruluştaki para akışını anlayarak, karmaşık bir kara para aklama soruşturmasında bireylerin rollerini belirleyebilir ve genellikle kuruluştaki kilit rakamları belirleyebilirsiniz.

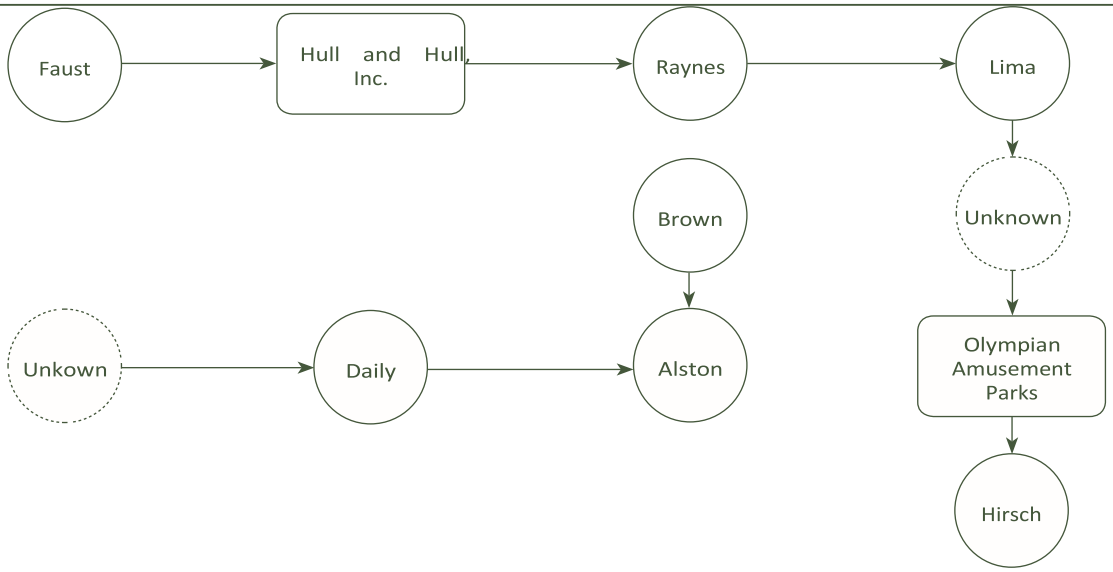
Bu bir uyuşturucu soruşturmasıyla bağlantılıysa, o zaman bu kişiler genellikle uyuşturucuların kendileri ile ilgilenmezler ve uyuşturucu hareketini veya kuruluş içindeki para akışını göstermek için ayrı çizelgeler oluşturulabilir. Çoğu durumda, metanın akışı, organizasyonun hiyerarşik yapısını gösterir ve bu da, organizasyonun güç temelinin anlaşılmasına yol açar. Akış şemaları, siyasi etki veya denetim kontrolü gibi soyut faaliyetleri göstermek için de üretilebilir.

Tüm çizelgelerde olduğu gibi, bunlar analistin hayal gücüdür, ancak hatırlanması gereken önemli faktör, bağlantı hattının akışı göstermek için bir ucunda veya her ikisinde bir ok ucuna sahip olmasıdır. Şekil 8-1'de bir akış şeması örneği gösterilmektedir; dikkat edin, emtianın doğasına dair henüz bir belirti yok, sadece grafik akışı var.

Şekil 8-1. Kişileri ve kuruluşları içeren bir akış şeması örneği



Şekil 8-2. Kuruluşları ve bireyleri içeren daha fazla akış şeması



Şekil 8-2, kimliği bilinmeyen iki kişiyi içermektedir. Grafik, emtianın Hirsch'e aktığı yolları gösterir.

Akış şeması analizi çeşitli amaçlar için uygulanabilir. Genellikle ilişkilendirme analizinin sonuçlarını tamamlamak ve doğrulamak için kullanılır. En yaygın alt kategoriler şunlardır:

" emtia akış analizi

" Aktivite akış analizi

" Olay akışı analizi

Mal akışı analizi, o faaliyetin anlamını belirlemek için insanlar, işletmeler ve yerler arasındaki mal veya hizmet akışına bakar. Bir komplonun doğası, bir grubun hiyerarşisi veya bir dağıtım ağının işleyişi hakkında fikir verebilir. Suçun nihai lehtarını veya onun adına satın alınan varlıkların nihai yerini gösterebilir.

Bir emtia akış şeması normal olarak emtiaya bir referansı ve/veya belirli bir işlemi tanımlayan herhangi bir sayısal değeri, örneğin para birimlerini veya "akış"ı temsil eden yön okunun etiketindeki ağırlığı içerecektir. Mümkün olduğunda, etkinliğin zaman aralığını belirtmek için tarihler de gösterilir.

Emtia akışı analizi, aşağıdaki gibi soruları yanıtlamayı amaçlar:

" Söz konusu emtianın en büyük miktarını kim elde ediyor?

" Metanın hangi (kime) sifonlandığı gösterilen yerler ve kişiler var mı?

" Suçlu bir hiyerarşi söz konusuysa, metanın akışı o grup içindeki ilişkiler hakkında bize ne gösteriyor?

Bir emtia akış şeması, genellikle bir suç örgütünün yapısını yansıtır veya ortaya çıkarır. Soruşturma altındaki suç faaliyetinin görünür ve daha gizli operatörleri ve yararlanıcıları hakkında fikir verebilir. Grubun doğası ve faaliyetinin kapsamı hakkında varsayımlarda bulunmaya yardımcı olabilir. Mal akış çizelgelerinin bariz kullanımları arasında çalıntı mal, rüşvet, uyuşturucu dağıtımı, kara para aklama uygulamaları yer alır.

Bir emtia akış matrisi, genellikle emtia akış çizelgelerinin manuel olarak oluşturulması için kullanılır. Telefon kayıt matrisine benzer şekilde hazırlanır (bkz. Bölüm 9). Eklenen veriler

ilgili kişiler ve/veya işletmeler arasında hareket eden malları veya para birimini yansıtır. Malın menşei olduğu kaynakların adları, matrisin üst kısmında veya sol tarafında aşağı doğru mantıksal bir sırayla düzenlenir. Daha sonra bunları, metanın alıcılarının adlarının mantıksal bir düzenlemesi izler. Alt ve sağ taraf, "başlangıç" ve "bitiş" toplamları için serbest bırakılır. Matrisin bu tasarımı, analistin belirli bir metanın çıkış noktasından varış noktasına akışını takip etmesini sağlar.

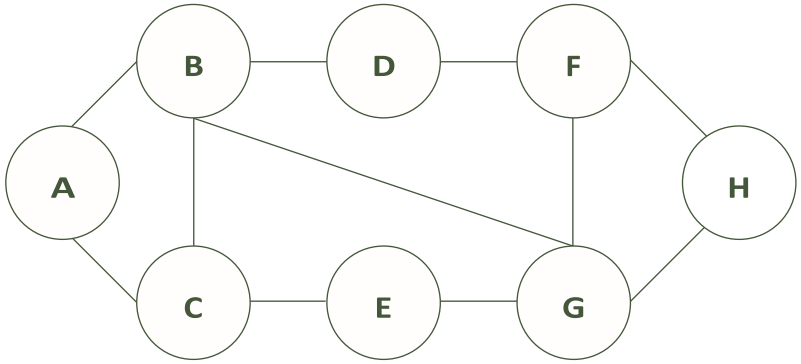
Bir akış şemasının oluşturulmasında iki yaklaşım vardır.

Yaklaşım 1:

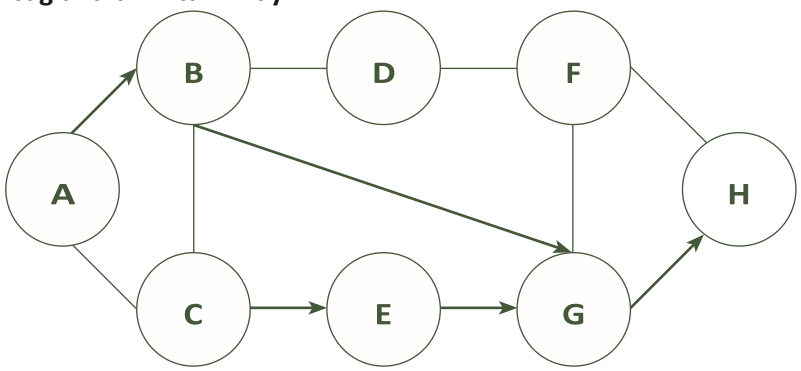
" Önce bir bağlantı şeması oluşturun;

" İlgilenilen malın akışıyla ilişkili bağlantıları belirleyin; " Bu bağlantıları kullanarak bir akış şeması oluşturun.

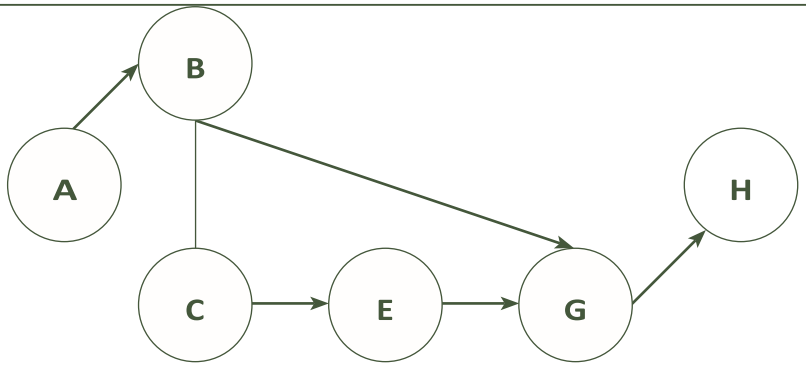
Şekil 8-3. Bağlantı şeması oluştur



Şekil 8-4. Akış bağlantılarını tanımlayın



Şekil 8-5. Akış şemasını çıkar



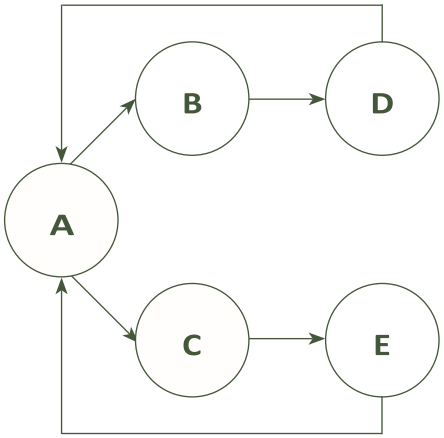
Yaklaşım 2:

- Tüm ham bilgileri bir araya getirin
- Hedeflenen malı belirleyin
- Bir kare ilişkilendirme matrisi oluşturun
- Bağlantı kodlarını matrise girin
- Bağlantı sayısını belirleyin
- Grafiği çizin; netleştirin ve gerektiği gibi yeniden çizin

Şekil 8-6. Akış bağlantı kodlarının girildiği kare matris

From	To					Totals
	A	B	C	D	E	
A		•	•			2
B				•	•	1
C	•					1
D	•					1
E	•					1

Şekil 8-7. Matriste yer alan bilgilerden oluşturulan akış şeması



Faaliyet akışı analizi , temel eylemlerin neler olduğunu belirlemek ve bir suça genel bir bakış sağlamak için bir dizi suç eyleminin veya operasyonel modalitenin genel bir görünümünü sağlamak için kullanılır. Bir faaliyet akış şeması, belirli bir süreci tamamlamak için gereken genel adımları gösterir. Olay akış şemasından farklıdır, çünkü ikincisi daha spesifiktir ve kesin

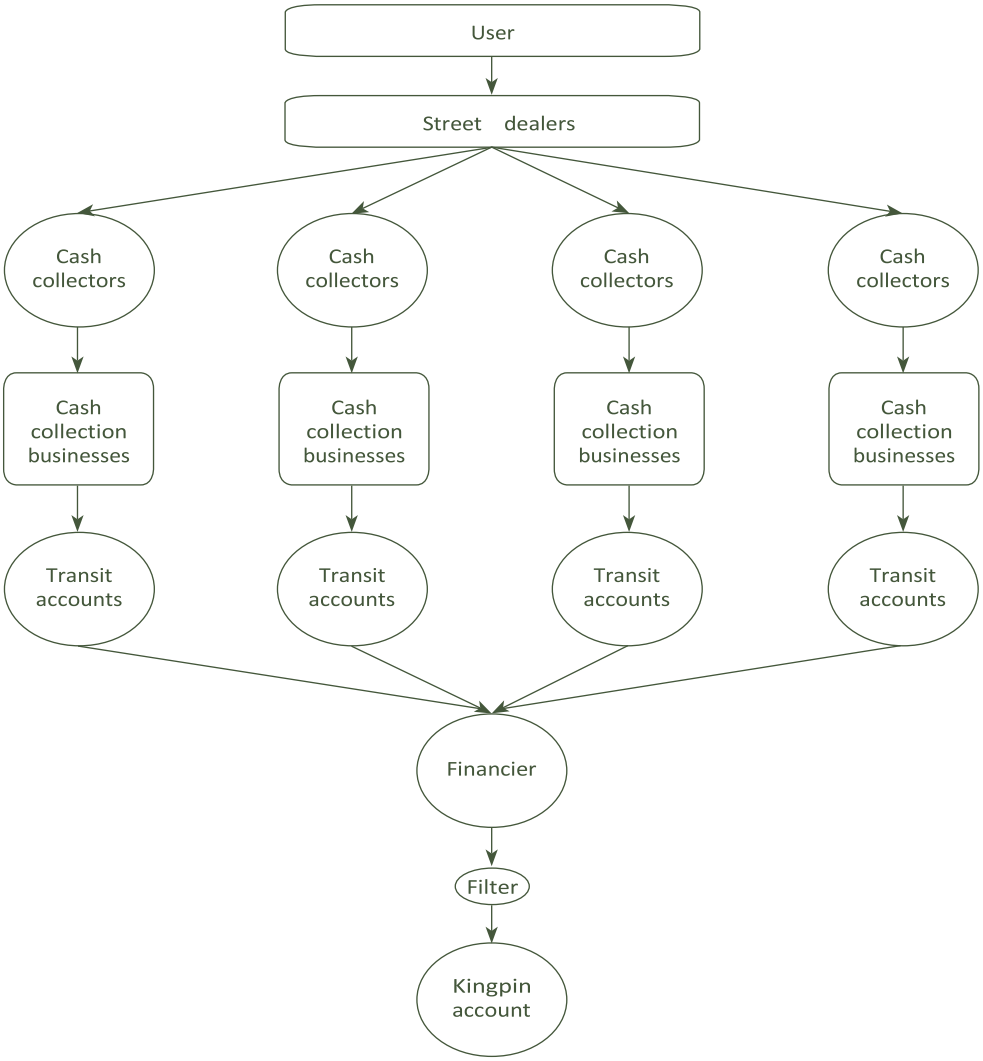
oluşumları ve tarihleri kullanır, etkinlik akış şeması ise olaylara genel bir bakış sağlar ve genellikle tarihleri kullanmaz.

Etkinlik akış çizelgeleri, bir süreçte veya benzer süreçler dizisinde meydana gelen olaylar hakkında bilgi toplayarak ve bunları belirli bir süreç yerine varsayımsal bir şekilde betimlemek için genelleştirerek yapılır.

Aktivite akış çizelgeleri, kara para aklama veya menkul kıymet manipülasyonu gibi karmaşık süreçleri açıklamak için kullanılabilir. Ayrıca, soruşturmaya duyarlı belirli bilgilerin incelenmemiş izleyicilere ifşa edilmesini önlemek için olay akış çizelgeleri yerine kullanılabilirler. Faaliyet akışı analizi, suçlar veya suç operasyonları arasında bir benzerlik veya bağlantı olup olmadığını görmek için bir karşılaştırma oluşturmak için de kullanılabilir.

Şekil 8-8. Örnek etkinlik akış şeması

Bir uyuşturucu kaçakçılığı organizasyonunda varsayımsal para akışı



Olay akışı analizi , analistin sonuçlar çıkarmasına ve/veya önerilerde bulunmasına izin vermek için zaman içinde meydana gelen olaylarla ilgili verilerin derlenmesi ve analizidir.

En sık olarak, ihlale yol açan ve ihlalden uzaklaşan olayların bağlam içinde görülmesi gereken belirli cezai ihlallerle ilgili olarak kullanılırlar.

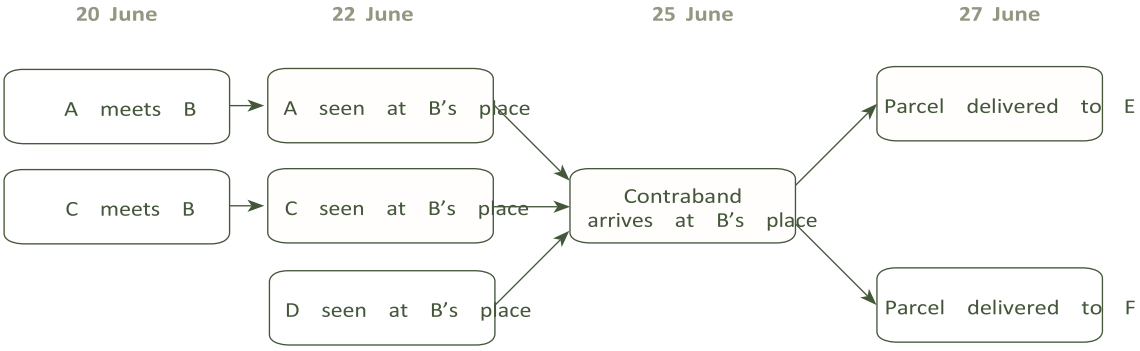
Olay akışı analizi, bir suç faaliyeti çerçevesinde meydana gelenlerin kronolojisidir. Yani, sadece suç faaliyetini etkileyen veya suç faaliyetinin bir parçası olan olaylar not edilmelidir. Bir olay akışı analizini tamamlamak için, meydana gelen olaylar için tüm vaka belgelerinin gözden geçirilmesi gerekir. Bu olaylar manuel bir deftere veya bilgisayarlı bir veri tabanına yerleştirilir. Harmanlama sistemi, verilerin tarihe ve gerekirse saate göre çıkarılmasına izin vermelidir. Uygun sıraya konduktan sonra, kronolojiye dahil edilmek için önemlerini belirlemek için olaylar gözden geçirilir.

Yapılan olay kronolojisi, bir sütunda olayın tarihini/saatini ve diğerinde olayın kısa bir açıklamasını gösteren bir olay çizelgesinde veya kronolojik bir tabloda görselleştirilebilir. Kronolojik tablolar, ticari olarak mevcut elektronik tablo programları tarafından rastgele verilerden otomatik olarak oluşturulabilir.

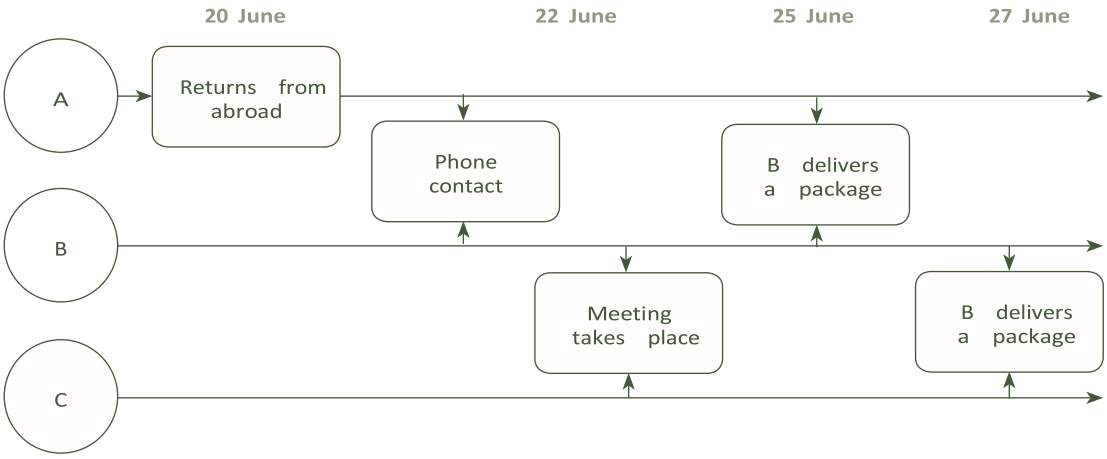
Olay akış analizi, bir dizi suçta meydana gelen olaylar benzer nitelikler açısından karşılaştırılırsa, işleyiş biçimlerinin belirlenmesiyle sonuçlanabilir.

Olay akış çizelgeleri basit veya matris olabilir.

Şekil 8-9. Basit olay akış şeması



Şekil 8-9. Matris olay akış şeması



Matris olay akış çizelgeleri, genel olarak matris olay çizelgelerine benzer şekilde, genellikle son derece büyük ve karmaşıktır ve en iyi ısmarlama bilgisayar yazılım paketleri kullanılarak oluşturulur.

9. Temel analiz teknikleri: telefon analizi

Telefon analizi, açıklayıcı ve faydalı sonuçlar üretebilen en yaygın tekniklerden birini temsil eder. Nicel veya istatistiksel analiz ve ilişkilendirme analizi olarak alt bölümlere ayrılabilir. Nicel analiz, bir telefon görüşmesinin sayısal parametreleri (gün, saat, süre) temelinde verilerde kalıplar oluşturmayı amaçlar. İlişkilendirme analizi, aramaların amacı ve içeriği, yani hedeflenen kişilerin ilişkileri ve temaslarının amacı hakkında hipotezler üretmek için istatistiksel analiz ve bağlantı şemalarının sonuçlarını kullanır.

Telefon verilerini yorumlamanın anahtarı, bunun basit bir yönlü veri biçimi olduğunu ve bu nedenle bu bölümde zaten kapsanan türlerin geleneksel akış şeması teknikleri kullanılarak çizelgelenmesi için ideal olduğunu kabul etmektir.

Telefon şirketleri tarafından müşterilerle olan normal işlerinin bir parçası olarak rutin olarak toplanan verilere, karşılaştırmalı kolaylık ve minimum kaynak harcaması ile erişilebilir. Bu tür bilgilerin belki de en önemli özelliği, müşteri tarafından serbestçe (ve dolayısıyla genel olarak gerçeğe uygun olarak) verilmesi ve müşteri ile doğrudan temasa gerek kalmadan telefon şirketlerinden alınabilmesidir. Ancak artık bu, suçluların rutin olarak farkında olduğu ve çevresini dolaşmaya çalıştığı bir süreçtir.

Burada tartışılanın telefon dinleme olmadığını vurgulamak gerekir. Bu teknikle, aramayı yapan veya alan kişinin kimliği veya aramanın içeriği hakkında hiçbir bilgi alınmaz.

Ancak üretilen, belirli telefonlar/telefon hatları arasındaki trafikle ilgili bilgilerdir.

Bu bağlantı türlerinin her biri (normal telefonlar, cep telefonları, çağrı cihazları, faks makineleri, bilgisayarlar, aslında herhangi bir iletişim bağlantı türü arasında) potansiyel olarak değerli bir bilgi kaynağını temsil eder, ancak bu "bilgi kaynaklarının çok sayıda ve çeşitliliği". ” araştırmacı için sorunlu olabilir. İlk olarak, analistin erişebileceği bilgilerin ayrıntıları kaynaklara göre değişir. Verilerin uyumsuzluğu ve farklı kaynaklardan almanın basit pratik zorlukları, özellikle zamanın bir faktör olduğu durumlarda, bilgilerin kullanılabileceği kullanımı bir dereceye kadar kısıtlar. Mümkün olan her yerde, veriler kağıttan değil yapılandırılmış elektronik formatta elde edilmelidir.

İkinci olarak, tedarikçilerinin müşteri veritabanlarının bilgisayarlaştırılması, veri koruması açısından başka prosedürel sorunlar yaratır.

Bu faktörlere rağmen, görüleceği gibi, telefon bilgilerini kullanmanın faydaları, özellikle telefon analizinin sonuçları diğer kaynaklardan analiz edilen bilgilerle birleştirildiğinde dezavantajlarından çok daha ağır basmaktadır.

Telefon analizi, analist ve araştırmacı için ne yapabilir?

- " Şüpheli bir telefon tarafından çevrilen ve diğer sorgulama hatlarını açabilecek telefon numaralarının tanımlanması
- " Denilen kalıpların ve ortak sayıların tanımlanması

" arama sıklığı
" Potansiyel olarak, ortakların tanımlanması
" Arayanın konumu (cep telefonları)
" Çok kaynak verimli olun

Analistler olarak şunu bilmelisiniz ki, telefonla analiz yapılması istendiğinde, bu tür verileri elde etmek için belirli yetkiler ve prosedürler mevcut olabilir, bu muhtemelen ülkeden ülkeye farklılık gösterebilir. Ayrıca her şirket verileri farklı formatlarda sağlayacaktır. Kursu tamamladıktan sonra kendi ülkenizin prosedürlerine ve irtibat noktalarına aşina olmanızı öneririz. Genel olarak, analist belirli bir telefon/abone hakkında belirli alanlarda aşağıdaki gibi bilgi edinmeyi bekleyebilir:

" Abonenin adı/adresi;
" Abonenin bağlantı numarası/numaraları;
" Abonenin hesap bilgileri;
" Ödeme detayları (banka/şube/hesap referansları);
" (belirli bir zaman periyodunda) yapılan bağlantıların, aşağıdakilerin ayrıntılarıyla birlikte eşzamanlı kaydı:
  - Aranan diğer numaralar;
  - Her aramanın saati, tarihi, süresi vb.;
  - Cep telefonu aramalarının direk konumları.

Açıkça bu bilgilerin çoğunluğu, ilgili kişilerden ziyade kuruluşlar (abone numaraları) arasındaki bağlantılarla ilgilidir. Bu bilgiyi daha iyi açıklamak için, bu nedenle, bir kare ilişki matrisi ve biraz değiştirilmiş akış şeması formu kullanılır. Temel akış şeması tekniklerine ve sembollerine küçük eklemeler kullanılır, böylece çizelge her bir bağlantı hakkında ek bilgileri sadece normal bir akış şemasında olduğundan çok daha net bir şekilde gösterebilsin, özellikle tek bir bağlantı çizgisi akışı görselleştirebilsin. ve her iki yönde de hacim bilgisi. Bu değişikliklere rağmen, bir telefon ücreti analiz çizelgesi, her bir bağlantıyı oluşturan bilgileri daha ayrıntılı olarak göstermek için uygun şekilde değiştirilmiş bir akış şemasıdır.

Analistin telefon bilgilerini tanımlamaya ve analiz etmeye başlamasını sağlamak için çoğu durumda en azından aşağıdaki ayrıntı gerekli olacaktır:

" Aramayı başlatan numara;
" Aramayı alan numara;
" Her iki yöndeki trafiğin sıklığı.

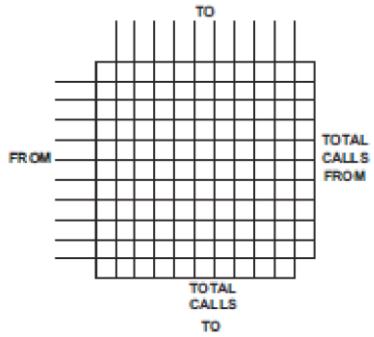
Analistin aboneler arasındaki her bağlantının yönünü hesaba katabilmesi için normal üçgen matris yerine kare matris kullanılır.

Başlatılan (abone tarafından yapılan) çağrıların telefon numaraları, karenin sol tarafında dikey (gelen) eksende listelenecektir.

Gelen aramaların (abone tarafından) telefon numaraları, karenin üst tarafında yatay (giden) eksende listelenecektir.

Bunu başarmak için, ilişki matrisi bir kare şeklini alarak biraz değiştirilir. Karenin sol tarafındaki dikey eksen, bir aramanın başladığını gösterecektir. Karenin üst tarafındaki yatay eksen, bir aramanın alındığını gösterecektir.

Şekil 9-1. Boş matris



Telefon bağlantı şeması aşağıdaki yedi adımla oluşturulabilir:

1. Tüm numaraları belirleyin (her zaman çevirme kodlarını kullanın)

Trafiğe dahil olan tüm telefon numaralarını belirleyin - gelen aramaların numaraları ve alınan aramaların numaraları.

2. Aboneleri düzenleyin (sayısal sırayla)

Alan kodu da dahil olmak üzere tüm sayıları artan sırada düzenleyin. Aynı alan koduna sahip birden fazla varsa, numaraları önce alan koduna göre düzenleyin, ardından her alan kodu içinde sıralayın. Farklı ülkelerden numaralar dahil edilirse, mevcut verilere tüm uluslararası kodların eklenmesini sağlamak için özen gösterilmelidir.

3. Aboneleri girin (Dikey)

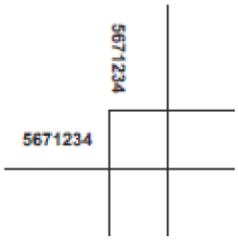
Tüm listeleri, en üstteki en düşük alan numarasından başlayarak, karenin sol tarafındaki dikey eksene girin. Matrisin en sol kenarındaki "from" gruplandırmasını etiketleyin.

4. Aboneleri girin (Yatay)

Tüm listeleri, karenin üst kısmındaki yatay eksende aynı sırayla girin. Matrisin üst kenarındaki gruplandırmayı "to" olarak etiketleyin.

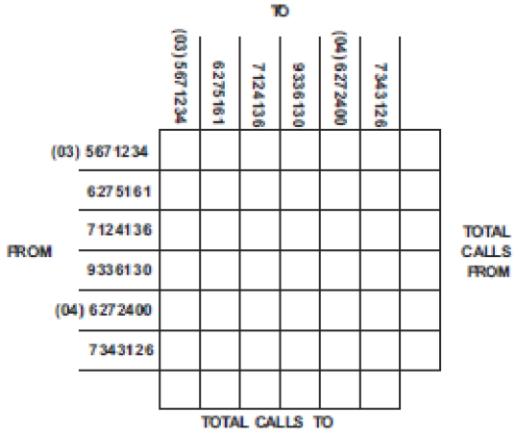
Dikkat: İlk sayının dikey eksendeki ilk sayı ile aynı olması için listeye karenin solundaki yatay eksen boyunca başladığınızdan emin olun.

Şekil 9-2. Tek sayılı matris



Şekil 9-2'de her bir sayının hem yatay hem de dikey eksenlerde nasıl aynı konumu işgal ettiğine dikkat edin. Tamamlanan matris, şekil 9-5'te gösterildiği gibi görünecektir.

Şekil 9-3. Tüm sayıları içeren matris



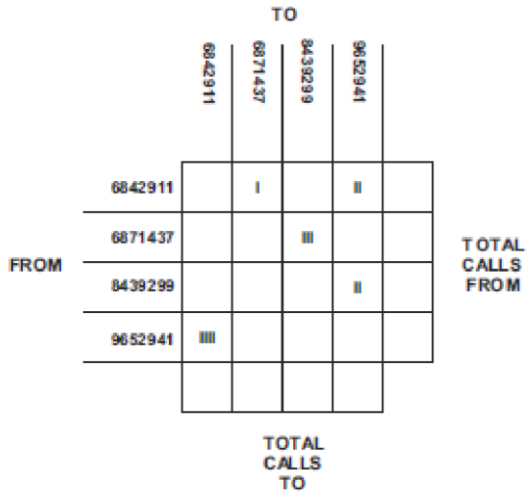
5. Çağrı sıklığını girin

Bir numaradan diğerine yapılan her aramayı, her iki listede de ortak olan matris hücresine küçük bir çetele işareti yaparak not edin.

Şekil 9-4. Örnek çağrı sıklığı tablosu

	Calling Number		Number Called	
Example	9652941	calls	6842911	Four times
	6871437	calls	8439299	Three times
	6842911	calls	9652941	Two times
	6842911	calls	6871437	One time
	84939299	calls	9652941	Two times

Şekil 9-5. Listelenen çağrılar için tamamlanmış ilişkilendirme matrisi



6. Her sayı için dolu karelerin sayısını ekleyin

Her bir numaranın (satır boyunca) kaç numarayı aradığını ve her numarayı (sütunda) kaç numaranın aradığını sayın. Sonuç, bitmiş grafikte bu numaraya bağlanması gereken

bağlantıların sayısını temsil eder. Grafik için bir başlangıç noktası olarak, en fazla sayıda bağlantıya sahip sayılar, tablonun ortasına yerleştirilmelidir.

7. Bir bağlantı şeması geliştirin

İlişkilendirme matrisinde yer alan bilgilerden bir bağlantı şeması geliştirin. Kişiler ve kuruluşlar arasındaki bağlantılarda olduğu gibi, farklı telefon numaralarını temsil eden sembolleri bağlamak için hatları kullanın.

Ancak telefon tablosuna, aramanın yönünü belirtmek için bir ok ekleyin. Örneğin, aramalar hem 01924-770792'den 0113-2928333'e hem de 0113-2928333'ten 01924770792'ye gittiğinden, oklar aşağıda gösterilecektir:

Şekil 9-6. Aramaların yönünü gösteren oklar

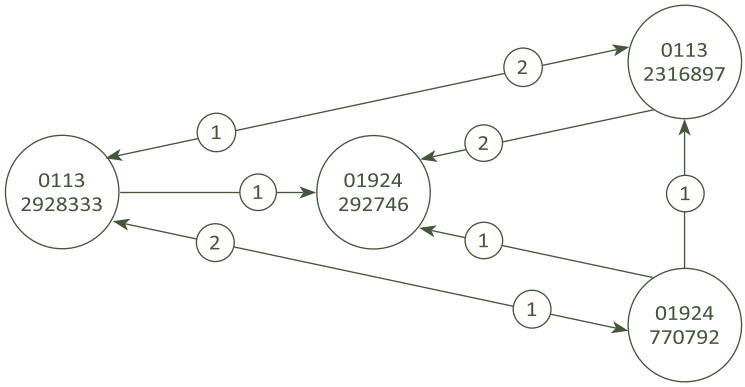
Çağrıların sıklığını (toplam sayı) göstermek için, okun hemen önündeki satıra küçük bir daire koyun ve yapılan çağrı sayısını ok yönünde girin. Bu, 01924-770792'nin 0113-2928333'ü iki kez aradığını ve 0113-2928333'ten bir çağrı aldığını gösterir.

Şekil 9-7. Bağlantı şemasında her iki yönü ve sıklığı gösterme

Şekil 9-8. Alternatif görüntüleme yöntemi

Yukarıdaki ilişkilendirme matrisinde yer alan bilgilerin bir bağlantı grafiğine dönüştürülmesi, aşağıdaki grafik şekil 9-9 ile sonuçlanır:

Şekil 9-9. Örnek ilişkilendirme matrisinin akış şeması

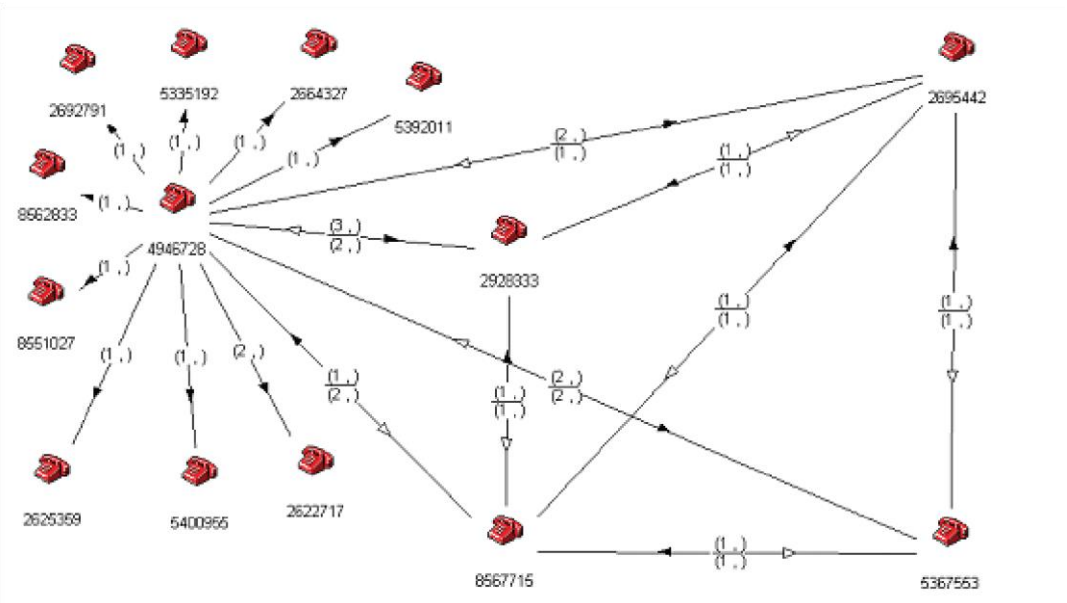


Bilgisayar tarafından oluşturulan çizelgeler

Telefon analiz çizelgelerinin elle oluşturulması, yalnızca en basit veri kümeleri için mümkündür. Analitik yazılım uygulamaları, bu ve diğer teknikler için artık suç istihbaratı alanında yaygındır. Bilgisayarların ve ilgili yazılımların kullanımı bu kılavuzun kapsamı dışında

olmakla birlikte, kullanılan teknikler aynıdır. Ne üretileceğine dair bir fikir vermek için bilgisayar tarafından oluşturulan bir telefon analiz tablosu dahil edilmiştir.

Şekil 9-10. Bilgisayar tarafından oluşturulan telefon analiz tablosu



Genel olarak telefon analizinin son yıllarda çok daha karmaşık bir süreç haline geldiğini de belirtmek gerekir. Çoğu zaman, Şekil 9-10'da gösterilen telefon analiz çizelgesi türü bile, mevcut veri hacimleri ve suçlular tarafından bu tür kanun uygulama tekniğine karşı sıklıkla benimsenen karşı önlemler ile ilgili olarak muhtemelen çok basit olacaktır.

Cep telefonu kullanan suçluların, arayanın kimliğini olabildiğince gizlemek için ön ödemeli kartlar ve el cihazlarını (IMEI numaraları) ve SIM kartları (IMSI numaraları) kullanmaları artık yaygın bir uygulamadır. Kullanıcılar arasındaki bağlantıları ortaya çıkarmak ve henüz bilinmeyen bir iletişim aracının nerelerde kullanımda olabileceğine dair göstergeler vermek için otomatik sistemler kullanan telefon görüşmelerinin modeline bakmak daha önemli hale geldi. Bu, çağrı merkezlerinin, ağ geçidi numaralarının vb. kullanımıyla daha da karmaşık hale gelebilir. Bir telefonu belirli bir kullanıcıya bağlamanın başka bir tekniği, iletişimin yapıldığı yerlere ve zamanlara bakmaktır.

10. Çıkarım geliştirme

GİRİİŞ

Bağlantı analizi gibi veri tanımlama ve entegrasyon teknikleri kendi başlarına bir amaç değildir. Daha önce tartışıldığı gibi, bunlar sadece analistin araçlarıdır; Analiz edilen bilgiden anlam çıkarma sürecindeki adımlar.

Analistin günlük çalışmasının ortak gereksinimi, bilgiyi toplayarak ve sonra parçalayarak, neyin "olduğu" ya da olabileceği hakkında bir anlam çıkarma ve bir teori veya teoriler geliştirme ihtiyacıdır. Analitik çalışmanın özü budur.

Kabul edilmesi gereken şey, herhangi bir tek bilgi kümesinin kaçınılmaz olarak anlamı hakkında birçok alternatif açıklama, teori ve hipoteze sahip olacağıdır. Bunlardan bazıları bariz ve/veya oldukça olası iken, bazıları çok uzak ve son derece olası görünebilir. Yine de analist tarafından seçenekler olarak tanımlanmaları ve değerlendirilmeleri gerekir.

Bu hipotezleri görselleştirmenin faydalı bir yolu, model türleridir. Modeller, çok daha büyük, daha karmaşık bir durumun yönlerini incelememize izin veren prototipler olarak kullanılabilmeleri açısından faydalıdır. Örneğin otomobil üreticileri, yeni/daha iyi araçlar veya özellikler için fikirlerini, daha sonra tüm aracı inşa etmekten daha hızlı, ucuz ve etkili bir şekilde test edebilecekleri modeller oluşturarak deniyorlar. Suç bilgileri hakkında hipotezler yaratarak, tıpkı bir otomobil üreticisinin yeni bir aracı test etmesiyle aynı şekilde fikirlerimizi, teorilerimizi "test sürüşü" yapabiliriz. Bu, teorilerimizin nasıl işlediğini, nasıl performans gösterdiğini, hangilerinin çalışıp hangilerinin çalışmayacağını ve birden fazla olduğu yerde hangisinin en iyi performansı gösterdiğini bulmamızı sağlar.

Bu da müşterilerimize kaliteli, test edilmiş istihbarat seçenekleri sunmamıza yardımcı olur, böylece daha az kaynak maliyeti ve daha az kaynak maliyeti ile objektif bir şekilde bilinçli seçimler ve kararlar alabilirler. daha büyük bir başarı şansı.

İşte düzenli olarak kullandığımız bazı "modeller" örnekleri:

" Prototip arabalar, uçaklar, makineler

Matematiksel modeller, denklemler

" İstatistikler/grafikler

" Analiz çizelgeleri

/ hipotezler/çıkarımlar

" Suçlu profilleri

" Şüpheli/istihbarat paketleri

/ misyon beyanları/operasyonel emirler/iş planları

" Taktik/stratejik vizyonlar/planlar/raporlar

" Örgütsel/siyasi politika

Tesisler

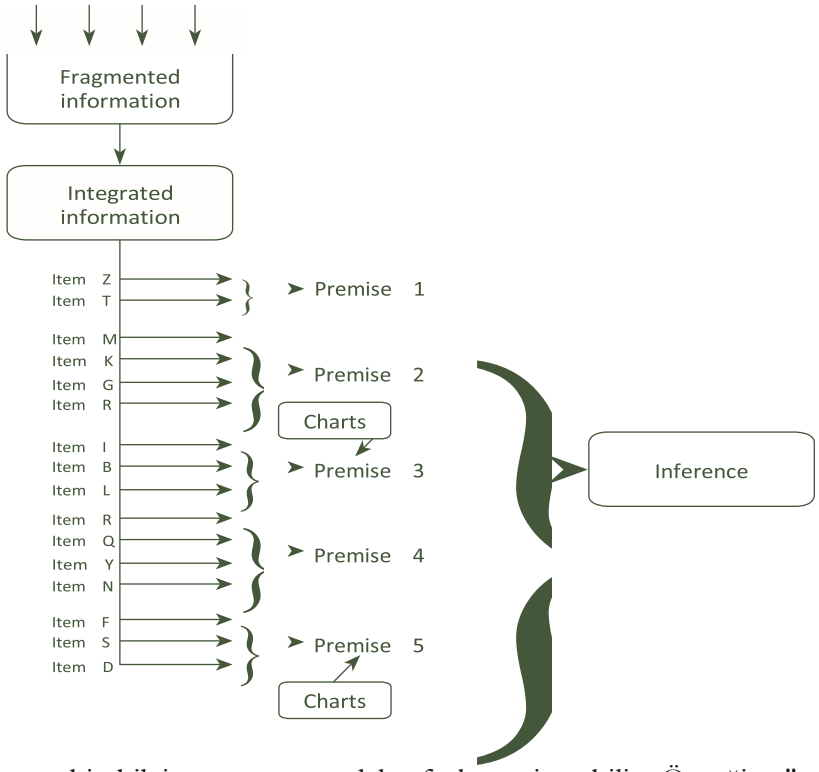
Öncülün sözlük tanımı şudur: "Temel veya argüman olarak hizmet eden önceki bir ifade".

Benzer şekilde, çıkarım geliştirmede bir "öncül", belirli bir noktaya değinmek için bir araya gelen gerçekleri veya bilgi parçalarını tanımlamak için kullanılır. Binalar, veri açıklamasına kıyasla gerçek veri analizi sürecindeki ilk ve kilit aşamadır. Öncüllerin nasıl tanımlandığını anlamak, hacim bilgisinden anlam çıkarmanın, bilginin bize ne söyleyebileceğini belirlemenin ilk aşaması olduklarından, çıkarımlar geliştirmek için çok önemlidir.

Bilgi bir organizasyona aktığında genellikle parçalanır ve bu nedenle analiz amaçları için bir dizi öncül geliştirilebilecek entegre bir forma kanalize edilmesi gerekir. Sonuç olarak bir çıkarım veya bir dizi çıkarım üretilebilir.

Bir veri öğesi, bir veya daha fazla öncülü destekleyebilir. Çoğu zaman çizelgeler, belirli bir önermeye daha fazla ağırlık vermek için de üretilir.

Şekil 10-1. Örneklem



Bir öncül, yalnızca bir bilgi parçası veya daha fazlasını içerebilir. Örneğin, "arabada" CD çalarların çalındığı Sandford bölgesinde motorlu taşıt hırsızlıklarının artmış olabileceği tipik bir varsayım olabilir. Bu sadece bir veya yüzlerce suç raporundan gelmiş olabilir; her iki durumda da öncül, yani sorunun tanımlanması aynıdır. Bilgi parçalarının sayısının (veya kalitesinin) yaratabileceği tek fark, o önermeye verilen değer veya önemdedir. Bu, daha sonra ele alınacak olan olasılık değerlendirmesinin rolüdür.

Bu aşamada iki noktayı anlamak çok önemlidir. İlk olarak, tesislerin açıklanan bilgilere en yakın bağlantı olduğu ve bu itibarla bu verilerin en objektif ve doğru temsili olduğudur. İkinci olarak, belirli bir bilgi kümesinden türetilen herhangi bir öncül kümesi için, öncüller farklı çıkarımlar önermek için farklı şekillerde birleştirilebilir. Bu, nihai bir çıkarıma varma sürecinin geçerli bir parçasıdır ve analizin tek bir seçenek yerine bir dizi seçeneği nasıl değerlendirdiğini ve değerlendirdiğini kanıtlar.

Tipik bir öncül aşağıda gösterilmiştir ve dört bilgi parçasından oluşturulmuştur:

1. Bilgi: Smith'in işi yok
2. Bilgi: Smith'in 400.000 £ değerinde bir evi var
3. Bilgi: Smith'in üç adet yüksek değerli spor arabası var
4. Bilgi: Smith lüks bir yaşam tarzına sahiptir

Önerme: Smith'in tanımlanamayan bir geliri var
Öncüller ve çıkarımlar mantıksal bir çerçeve içinde geliştirilir. Bu çerçevenin unsurları bir argüman ve mantıktır.

Argüman: Her biri önemli bir bilgi veya önermeyi yansıtan ifadeler veya gerçekler listesi. Bu ifadelere öncül denir ve birbirine bağlandığında çıkarıma yol açar.

Mantık: Çıkarımı oluşturmak için öncüllerin ve çıkarımların birbirine bağlanma şekli.

çıkarım

Herhangi bir cezai soruşturmada analizin amacı, bilginin ne anlama geldiğine dair bir açıklama bulmaktır. Bu açıklama bir çıkarım olarak bilinir. Çıkarım, neler olup bittiğini kısaca açıklayan bir ifadedir. Daha resmi olarak, bir çıkarım, mantıksal düşüncenin ürünüdür.

Analistin nihai hedefi, soruşturulan suç faaliyetinin doğası ve kapsamı ve dahil olan belirli kişi ve kuruluşlar hakkında çıkarımlar geliştirmektir. Bununla birlikte, bir çıkarımın, olası doğruluğuna ilişkin bir tahmin olmaksızın sınırlı bir değere sahip olabileceği kabul edilmelidir.

Bir çıkarıma tepki verme şeklimiz, onun doğruluğundan ne kadar emin olduğumuza bağlı olarak değişecektir. Örneğin, nispeten düşük bir güven düzeyine sahip olduğumuz bir çıkarım, yalnızca ek bilgilerin toplanmasını yönlendirmeye hizmet edebilir. Öte yandan, yüksek düzeyde bir güven, suç faaliyetinin esaslarını hedef alan belirli eylemlere yol açabilir.

Ceza soruşturmasının doğası gereği, herhangi bir ceza soruşturmasında mevcut olan bilgiler neredeyse her zaman eksiktir ve soruşturma ilerledikçe sürekli değişir. Sonuç olarak, belirsizlik karşısında çıkarımlar yapılır ve bu nedenle analistin umabileceği en iyi sonuç, gerçeğe mümkün olduğunca yakın bir çıkarımdır.

ÇEKİM TÜRLERİ

Dört tür çıkarım vardır:[2]

Hipotez: Geçici bir açıklama; doğrulama veya reddetme için ek bilgi gerektiren bir teori.

[2]Tüm çıkarım türleri test gerektirir.

Tahmin: Gelecekte olacak/olabilecek bir şey hakkında bir çıkarım.

Tahmin: çıkarım , örnek: para miktarı , gerekli süre, işlem boyutu ve yakında.

Çözüm: İyi desteklenen bir açıklama; hipotez, tahmin tahmin etme şu şekilde:

- Doğrulanması muhtemel görünüyor
- Onaylama önceliği
- Tümü oluşturan hipotezler, tahminler ve/tahminlerden kaynaklanan sonuçların temsili bir özetidir.

İlk çıkarsama, büyük olasılıkla, veri toplamaya yönlendirilebilecek olan bir varsayım varsayımıdır.

Eğer hemen bir sonuca varmak mümkünse, o zaman sorun muhtemelen gerekli olan küçük analiz veya ilk etapta.İleri veri toplama veya örnekleme istihbarat süreci etrafında bir veya daha fazla kez, çıkarımınızın kalitesini iyileştirmenize izin verir. Bununla birlikte, bir noktada, sonuçsuz bir çözümleme, dağılmadan elde edilir.

Çıkarım geliştirme sürecindeki son adım , olasılık değerlerinin kullanılmasıdır.[3]

Olasılık, "olayın meydana gelme sayısı" ile "olayın meydana gelmesi için fırsat sayısı" arasındaki oran olarak elde edilir.

vardır :

" *Geçmiş" olayların göreli "sıklığı"* —birçok zaman diliminde bile fazla verili olduğu yerde, geçmişte meydana gelen olası olaylara bir kılavuz olarak kullanılır.

" *Teorik" tahmin* —her ne kadar türetilmiş olursa olsun, belirli bir formülün öngörü için kullanıldığı durumlarda.

" Öznel *" tahmin —tahmin* yalnızca kişisel görüşe veya yargıya dayandığı yerde, genellikle bir deneyim, uzmanlık veya konum olarak bir ayrıcalıktır.

türleri :

" *" Basit* —bir olayın meydana gelme olasılığı

" *" Ortak — iki olayın aynı* anda meydana gelme olasılığı

" *" Koşullu* —birinci olayın meydana gelmesine bağlı olarak, bir ikinci olayın olasılığı

Bu son kavram, tümevarımsal mantık süreci boyunca geliştirilen çıkarımları değerlendirmek için kullanılır.
Öncüller , çıkarıma götüren yapı taşlarıydı. O halde, bunlar ayrıca, olasılık tahminlerinin dayandırılması gereken yapı taşlarıdır .

[3]Olasılık atamaya, özellikle de kanıta dayalı kısıtlamalara son derece dikkat edilmelidir.

öncül mantıksal olarak çıkarımın doğru olma olasılığını artırır. Örneğin, yalnızca bir öncülün doğru olduğu varsayıldığında, çıkarımın yüzde 10'luk bir doğru olma şansı olabilir. İki öncülün doğru olduğu varsayıldığında, olasılık yüzde 15-25'e yükselebilir, vb.

Suç soruşturmaları, hipotezlerden yararlanırken, bunlar, soruşturmanın genişletilebileceği yönlere işaret eden fikirler ve içgörüler sunar. Hipotezler, araştırma ekibi için çalışan fikirleri temsil eder ve endüktif mantığın ürünü olmaları gerekir. Yalnızca araştırmalardan çıkan sonuçların muhasebeleştirilmesi değil, araştırma ekipleri için değerli sonuçlar üreten yaratıcı düşüncedir.

Stratejik istihbaratta, hipotezler ve çıkarımlar, etkili uzun vadeli eylemlerin planlanmasına ve hazırlanmasına izin vermek için suçlu düşmanların niyetleri, olasılıkları, sınırlamaları ve savunmasızlıkları ile ilgili konulara odaklanır. Operasyonel analizde hipotezler ve çıkarımlardan temel fark, anında operasyonel kullanıma konabilecek özel durumla ilgili konularla ilgilenmeleridir.

Hipotezler ancak ek bilgilerin toplanması yoluyla kabul edilebilir, değiştirilebilir veya reddedilebilir. Hipotezleri test etmek için bilgi toplanması, göstergelerin geliştirilmesine önceden bir miktar düşünüldüğünde en etkili şekilde yapılır. Göstergeler, önceki varsayımları destekleyen veya reddeden belirli olaylara işaret eden ipuçlarıdır.

Analiz süreci boyunca yapılan tüm araştırmalardan yararlanarak ve bağlam içinde hipotezlerin geliştirilmesi ve test edilmesi, nihayetinde sonuçların veya önerilerin taslağının oluşturulmasıyla sonuçlanmalıdır. Çalışmanın özünü ve bundan kaynaklanan içgörüleri operasyonel veya yönetimsel sorumlulukları olan taraflara ilettikleri sürece, analitik bir ürünün hayati bir unsurudurlar.

YANLIŞ MANTIKTAN KAYNAKLANAN YANLIŞLAR

Çıkarım geliştirmeye mantıklı bir yaklaşım benimseyen analist, yanlış çıkarımlarla sonuçlanabilecek mantıksal hatalardan veya safsatalardan kaçınmalıdır. En yaygın yanılgılar iki genel sınıftan birine girer.

İhmal yanılgıları: bir argümanın bazı önemli öncülleri, değerlendirmeleri veya yönleri atlanmıştır:

- *Aşırı basitleştirme* —ilgili tüm koşulları veya olasılıkları yeterince açıklayamayan bir çıkarım.
- *Yetersiz örnekleme* — çok az bilgiden veya temsili olmayan bilgilerden çıkarımlar (tahminler) yaparak üretilen bir yanılgı.
- *Hatalı neden* —aynı anda var olan veya birbirinden önce gelen olaylar veya koşullar arasında kurulan yersiz bir sebep-sonuç ilişkisi— korelasyon mutlaka sebep ve sonucun varlığı anlamına gelmez.
- *Yanlış ikilem* —yalnızca aşırı alternatiflerin dikkate alındığı bir yanılgı.

Yanlış varsayımlar:

- *Soruya* yalvarmak —soruya ya da soruna yanıt vermek yerine, soru yeniden ifade edilir ya da sorun değiştirilir.

" *Gerçeğe aykırı hipotez* - birisi koşullar farklı olsaydı ne olacağını kesin olarak belirttiğinde ve doğrulanamayan bir hipotez sağladığında ortaya çıkan bir yanılgı.

" Yanlış kullanılan *analojiler* - bir analojiden akıl yürütürken, gerçek dünyadaki nesne veya olayın bir analojideki nesne veya olaya benzer olduğu varsayılır. Analojiler, analitik çalışmada kanıt veya kanıt olarak uygun değildir.

Bir analistin diğer bir sorumluluğu, belirli bir prosedürün veya araştırma hattının yürütülmesiyle ilgili riskleri değerlendirmektir. Operasyonel bir eylemin kaynak maliyetini, bu eylemin ele almayı amaçladığı bir suç sorununa karşı dengeleme ihtiyacı olduğunda, risk analizi giderek daha önemli hale geliyor.

İyi bir çıkarım tipik olarak, kilit bireylerin "kim" olduğunu, "neye" dahil olduklarını, "nerede" çalıştıklarını, "neden" yaptıklarını, "nasıl" yaptıklarını ve mümkünse" içermelidir. ne zaman" tekrar saldırmaları muhtemeldir.

Bir Çıkarım örneği aşağıda gösterilmiştir:
Stephen James, çalıntı mallar için hafif uyuşturucu ve sahte para takasını içeren bir suç operasyonunun başıdır. Sahtecilik, uyuşturucu ithalatı ve hile yoluyla mal elde etme, James ve ortaklarının finansal kazanç sağlamak için kullandıkları başlıca yöntemlerdir. Son iki yıldır Sandford bölgesinde faaliyet gösteriyorlar.

Mantık

Amaçlarımız için iki tür mantık vardır, tümdengelim ve tümevarım.

Tümdengelim mantığı: Tümdengelim mantığı tamamen gerçeklere dayanır. Gerçeklerin ötesine asla geçmez. Öncüller gerçeklere dayanır ve çıkarım öncüllerin ötesine geçmez. Dolayısıyla, öncüllerin dayandığı olgular doğruysa, çıkarımın da doğru olması gerektiği sonucu çıkar. Argüman, genel koşuldan belirli koşullara doğru ilerler.

Tümdengelim mantığı örneği:

Önerme: Çalınan malları elleçlemek mahkumiyetle cezalandırılan bir suçtur.
Önerme: Sam Sharpe çalıntı malları kullanmaktan suçlu bulundu.
Saldırganlık : Sam Sharpe, çalıntı mallarla uğraştığı için cezaya tabidir.

Tümevarımcı mantık: Tümevarımcı mantık aynı zamanda gerçekleri de inceler, ancak tümdengelim mantığının aksine, bu gerçeklerin ötesine geçer, analist parçalardan bütüne veya ayrıntılardan genele çalışmak için akıl yürütmeyi kullanır.

Yine tümdengelim mantığının aksine, tümevarım mantığı gerçeklerin ötesine geçtiği için, öncüller doğru olsa bile çıkarımın doğru olduğuna dair mutlak bir garanti yoktur. Suç araştırmacıları olarak, öncüller doğruysa, çıkarımın muhtemelen doğru olduğu durumlarla ilgileniyoruz.

Endüktif mantık örneği:

Önerme: Mike Lee ve Chris Wilson hapishanede hücre arkadaşıydılar ve şimdi birlikte yaşıyorlar.

Önerme: Mike Lee yakın zamanda tutuklandı ve evlerinden kontrollü uyuşturucu tedarik etmekten mahkum edildi.

Çıkarım: Chris Wilson, kontrollü ilaçların tedarikinde yer almaktadır.

11. Sonuçların sunumu

LOJİK BRİFİNGLER VE YAZILI RAPORLAR

sözlü brifingler

Sözlü brifing en çok, acil eylem için temel oluşturacak bir analize genel bir bakış sunmak için kullanıldığında etkilidir - örneğin, kritik bir hızlı hareket durumunda sonuçların dağıtılması gerektiğinde. İzleyicilerin kendileri stilden etkilenir, etkili sunum analitik bir ürünün alınmasını büyük ölçüde etkileyebilir.

Tanım: Bir durumun temel unsurlarının kısa bir sözlü sunumu veya belirli bir kitleye bir analiz.

Sözlü brifingin başlıca avantajı, analizin kullanıcıları ve üreticileri arasında yüz yüze etkileşim sağlamasıdır. Analiz ürünleri karmaşık olabilir; Etkili bir sözlü sunum, sonuçları net bir mantıksal sırayla azar azar iletme fırsatı sunar. Bu nedenle, brifinglerin, onları üretmek için yapılan analize giren mantıksal akıl yürütmeyi yansıtması çok önemlidir.

Sözlü brifinglerin üç ana avantajı vardır:

" Zaman tasarrufu—en kısa sürede maksimum miktarda bilgi iletilebilir.

" Doğrudan temas—sözlü brifing analist ve müşteri arasında doğrudan temas sağlar. Bu, veri kaynaklarının dinamik olarak sorgulanması, veri güvenilirliğinin değerlendirilmesi, çıkarımlar ve olasılıkları vb. için bir fırsat yaratır. Hem müşteri hem de analist bunu kullanabilir Projenin doğru yönde ilerlemesini ve eyleme geçirilebilir sonuçlar üretmesini sağlama fırsatı Kullanıcı, doğrudan temas kurarak, konuyla ilgili diğer bilgilerle ilgili olduğu için analiz sonuçlarının önemini daha doğru bir şekilde değerlendirebilir.

" Dinamizm—sözlü brifing, en son bilgileri içerecek şekilde en son anda revize edilebilir. Bir projedeki gelişmeleri neredeyse gerçek zamanlı olarak iletebilir. Brifing aslında o ana kadar durumun bir açıklaması olabilir. brifingden hemen önce.

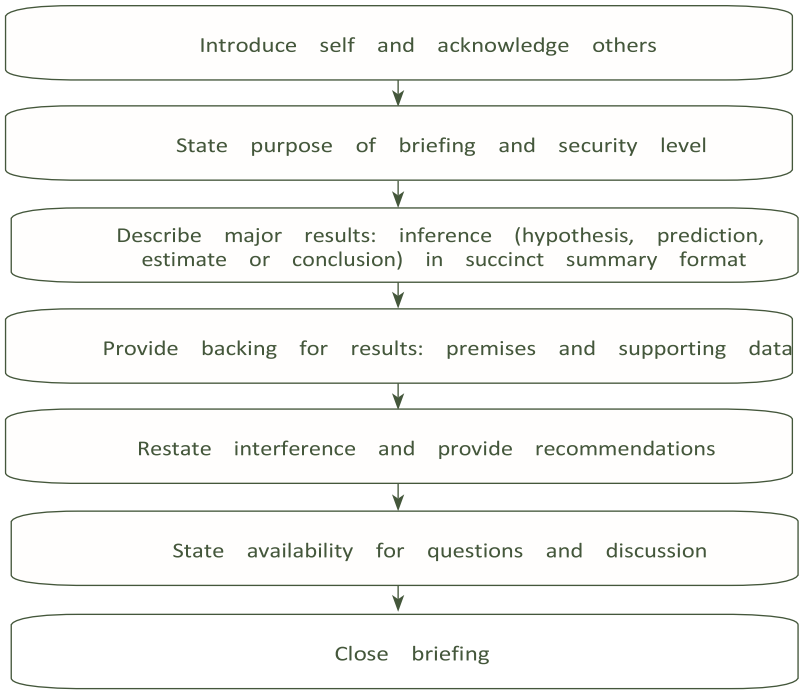
Sözlü brifingler, iyi bir doğaçlama ölçüsü ve yerinde düşünmeyi içerir. Bununla birlikte, istenen etkiyi yaratmak için bir brifingin önceden tasarlanmış bir senaryoyu izlemesi gerektiğinden, hazırlık yine de gereklidir.

Başlangıç olarak, dinleyicileri analiz etmek her zaman önemlidir - brifing sırasında verilen bilgiler ne için kullanılacak? İzleyicinin bilgi düzeyi nedir ve ilgi alanları öncelikli olarak nerede bulunur?

brifing yapısı

Dikkatli hazırlık ve mantıklı sunum, sözlü brifingin etkinliği için çok önemlidir. Analizinize giren mantıksal akıl yürütme, brifingde açık olmalıdır. Şekil 11-1, bu mantıksal akıl yürütmeyi yansıtmanın bir yolunu sağlayacak olan brifing için yapısal bir sıralamayı göstermektedir.

Şekil 11-1. Brifing sunumunun sırası



BRİFİNİN HAZIRLANMASINDAKİ KRİTİK ADIMLAR

İzleyiciyi analiz edin

Kitlenizin ihtiyaçlarını bilin. Örneğin, daha fazla yaygınlaştırma, karar verme, bir veri toplama planı geliştirme veya başka bir amaç için mi kullanılacak?

İzleyicilerdeki kişilerin rollerini ve sorumluluklarını aklınızda tutun ve tarzınızı ve içeriğinizi buna göre ayarlayın. (Diğer bir deyişle, bir Kıdemli Soruşturma Görevlisine (SIO) parmak ucuyla arama yapan bir grup memura sunum yapmanın farkını düşünün.) çok fazla gereksiz veri veya yetersiz ayrıntı sunmak.

Güvenlik konularını, özellikle mevzuat kapsamındaki görevlerinizi, diğer bir deyişle, izleyicilerin bilmesi gereken veya bilmelerine izin verilen bilgileri göz önünde bulundurun.

Kendinize "içerik, izleyici, çevre ve son olarak sizin için en iyi dağıtım yöntemi bu mu?" diye sorun.

Brifinginizi özetleyin

Çıkarımlarınız ve analitik süreçte çıkarımı geliştirdiğiniz öncüller, brifing taslağınız için mükemmel bir temel sağlar. Analiziniz ve sunumunuz arasında mantıklı bir süreklilik sağlarlar.

Anahat dört ana bölüm içermelidir:

- giriiş
- Çıkarım beyanı
- Destekleyici tesisler ve veriler
- Öneriler

Giriş: Giriş kısa olmalı ve brifingin amacını belirtmelidir. Kendini tanıt. Brifingdeki bilgilerle ilgili her türlü hassasiyet bu noktada belirtilmelidir. Gerektiğinde teşekkür de bu noktada yapılır.

Çıkarım beyanı: Kitleniz başlangıçta analizinizin sonuçlarını bilmek ister. Bu noktada analizin ayrıntıları ve ayrıntıları olmadan çıkarımınızı açıkça belirtin.

Destekleyici tesisler ve veriler: Tesisleriniz, brifinginizin bu bölümünün temelini oluşturur. En etkili olmak için, analitik süreç sırasında geliştirilen ve tesise ulaşmada en faydalı olan uygun çizelgeleri kullanmanız gerekir.

Çıkarımı yeniden ifade edin: Hedef kitlenize büyük resmi hatırlatmak ve önerilerinizi yapmadan önce onlara odaklanmak için.

Öneriler: Hedef kitlenize ek veri toplama gereksinimleri ve uygun olduğunda eylemler için diğer seçeneklerle ilgili öneriler sunun. Bu, kendi bilgi ve deneyiminizi verebildiğiniz ölçüde yapılacaktır. Tercih ettiğiniz bir seçeneğiniz/seçenekleriniz varsa bunu gerekçelerinizle birlikte belirtiniz. Sorular için zaman tanıyın.

Brifinginizi "kuru çalışma"

İçerikteki zayıflıkları, mantıksal sırayı, brifing yardımcılarının uygunluğunu, yardımcıları kullanımınızı, yaklaşımınızı ve sunumunuzu ve zamanlamanızı belirtmek için yetkin bir veya iki kişiye ön sunum yapın. Mümkünse mekan örneğinizi kontrol edin: TV ve video nasıl çalışıyor? Fişler ve ışık anahtarları nerede?

Brifing yardımları

Brifing yardımları sadece bunlardır; kendi ayakları üzerinde durmayacaklar. Açık, özlü ve mantıklı bir şekilde sunulan bir brifing sağlamada değerli araçlardır. Amaçları konuşulan kelimeyi güçlendirmektir. Genellikle, bir tepegöz, kağıt tahtası veya bilgisayar tabanlı sunum yazılımı ile kullanılan asetatlar gibi konuşulan sözcüğü destekleyen görsel sunumlardan oluşurlar.

Tip	İçin uygun	Dikkat edilecek noktalar

Flipchart KISA MESAJLAR 30'a kadar olan gruplar Kurşun kalemle çizilmiş çizgiler, siyah veya mavi kalın kalemler kullanın.Önceden hazırlık gerekli		
Flipcharts/Beyaz Tahtalar	TARTIŞMALAR	Basit tutun.
Tepegöz	AÇIKLAMALARLazer baskılı slaytlar en iyi kaliteyi verir.	
Projektör Gruplarının büyütülmesi gerekebilir.		
(OHP) slaytlar	Çoğu ihtiyaç Odada çok fazla gün ışığı varsa, renkli slaytlar iyi görünmez.	
İKNA EDİCİ	Yalnızca kısa klipler (8-10 dakika).	
	30 kişiye kadar gruplar	
Sinema tarzı olmadıkça video Resimler hareketli olmalıdır.		Doğru bir şekilde işaretlenmelidir.
	Ekipman Dikkat: Sayaç numaraları farklı kullanılabilir.VCR'lerde farklı çalışır.	
	SUNUM	
Bilgisayar-uzaktan sunum sırasında aydınlatma kısılmalıdır.	ile kullanıldığında açık ara en profesyonel olana kadar dayalı Gruplar yazılım çoğu şey	. Kullanım
Bildiriler	EK MALZEME Sunuma dahil değil ONAYLA KONSOLİDASYON	Yazılı veya basılı olmalı ve çok uzun olmamalıdır. Sözlü olarak verdiğiniz mesajı güçlendirebilir ancak diğer görsel araçlarla çelişmemelidir. İçeriğin yazımını, doğruluğunu ve alaka düzeyini fiziksel olarak kontrol edin ve hedef kitleniz için yeterli sayıda kopyanız olup olmadığını kontrol edin.

Not: Herhangi bir görsel yardımla, gösterim süresi boyunca ilgi odağı haline geldiklerini unutmayın. Yardım edeceklerse onları kullanın. Sunumunuz olmasına izin vermeyin - bilgisayar destekli slaytlar kullanıyorsanız özellikle tehlikelidir.

"Bir resim bin kelimeyi boyar" sözü olmasına rağmen, görsel yardımlar, eğer sunumla alakalı değilse veya sunuma zarar vermiyorsa hiçbir işe yaramaz. Görsel yardımcılar sunumunuzu tamamlamalı, onun yerini almamalıdır.

Ev yapımı görsel yardımcılar, dikkat dağıtıcı bir mayın tarlası olabilir, ancak iyi olduklarında büyük bir etki yaratırlar. Bunları oluştururken tanınan temel kurallar, postada listelenir.

Tepegöz asetatları

" 6,7,8 kuralını hatırlayın: En az 8 mm yüksekliğinde harfler kullanarak şeffaflık başına 7 satır olacak şekilde satır başına maksimum 6 kelime yazın.
" Ortalanmış veya sola yaslanmış tutarlı bir biçim ve düzen kullanın.
" El yazısı asetatlar için kalıcı kalemler kullanın. Bir damla su veya ter, su bazlı olanlarla saatlerce çalışmayı mahvedebilir.
" Karmaşık diyagramlar oluşturmak için bindirmeleri kullanın.

" Bir şeffaflığa birden fazla fikir koymayın.
" ham rakamlar" olarak sunmayın—ilişkileri göstermek için pasta grafikler, çizgi grafikler, çubuk grafikler kullanın.
" Kitaplardan veya diğer belgelerden sayfalar kullanmayın.
" Kenara çizmeyin veya yazmayın, en az 10 mm kenar boşluğu bırakın.

Sunumlar

" Farklı renklerde büyük harfler kullanarak yazdırın.
" Önce ince kurşun kalemle diyagramlar veya düzenler çizin; izleyicileriniz bunları görmez.
" Yazılı kelimeyi satır başına 8 kelime veya sayfa başına 8 satır olacak şekilde tutun.
" Tam cümleler değil, yalnızca madde işaretleri yazın.

Bilgisayar ve dijital projektör

Microsoft PowerPoint gibi mevcut yazılımlar, sözlü brifingler geliştirmek ve sunmak için verimli ve etkili bir yol sağlar. PowerPoint gibi uygulamalar, sözcük işleme, anahat oluşturma ve sunum araçlarını çizme içeren eksiksiz bir sunum paketi sağlar. Sunumlar 35 mm'lik slaytlardan, tepegöz asetatlarından veya doğrudan elektronik projektörlü bir bilgisayardan yapılabilir.

Brifing yardımı kullanımına örnekler

Aşağıdaki örneklerdeki baskı boyutu, elle basılan asetatlar için minimum olarak kabul edilmelidir.

Çıkarımınızı geliştirirken her zaman doğrudan, olumlu terimler kullanın. "Olabilir", "olabilir", "muhtemelen" gibi kelimelerden kaçının. Kesinlik derecesi olasılık değerine yansır.

Bir çıkarımın sunumu için görsel yardım örneği

" Mali kazanç için bu alanda büyük bir kokain ithalat ve dağıtım organizasyonu faaliyet göstermektedir.

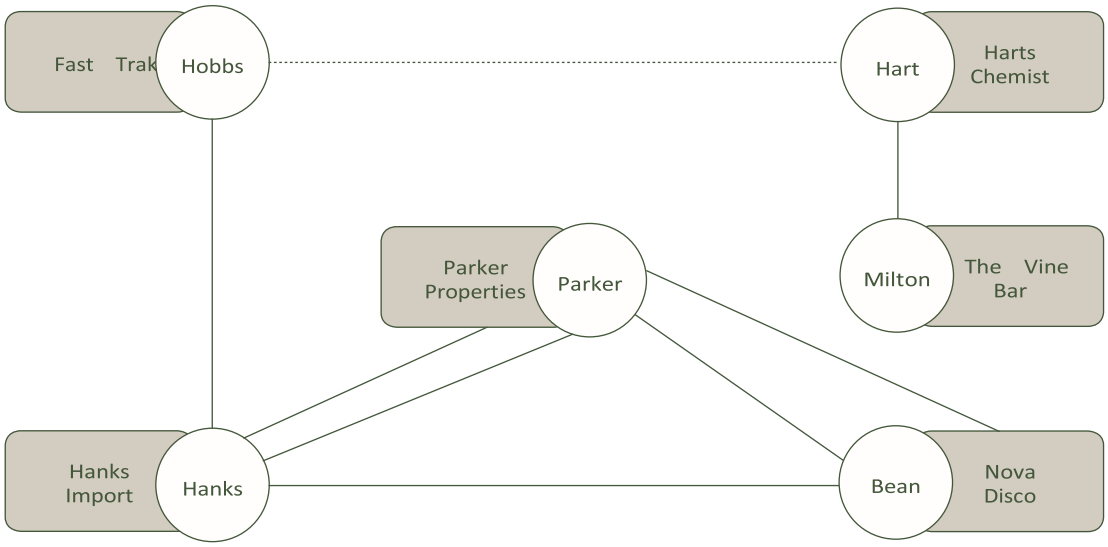
" Operasyonu kolaylaştırmak için meşru işletmeler ve bunların içindeki ortaklar kullanılıyor.
" Paul Parker bu organizasyonun başıdır.
" Bu hipotezin doğru olma olasılığı yüzde 70

Tesislerin sunumu için görsel yardım örneği

" Bu alanda mevcut kokain miktarında belirgin bir artış olmuştur.
" Güney Amerika'dan mal ithalatı ve dağıtımında birkaç yeni şirket kuruldu.

" Paul Parker, bu işletmelerdeki bireylerle bağlantılıdır
" Paul Parker, bu alanda uzmanlaşmış işletmelerle bağlantılıdır
" Bu üyelerin hepsinin uyuşturucuyla ilgili mahkumiyetleri var.

Şekil 11-2. Paul Parker ve ilgili ticari kuruluşlar arasındaki bağlantıları gösteren görsel yardım



Önerilerin sunumu için görsel yardım örneği

1. Operasyona halihazırda ve karşılıklı işbirliği amacıyla bakıp bakmadıklarını belirlemek için Gümrük ile irtibat kurun
2. Paul Parker'ın bağlantılı olabileceği diğer işletmeleri tanımlayın
3. İlgili şirketlerin başka şahıslar için de ilaç ithal edip etmediğini/dağıttığını tespit edin.
4. Operasyondaki kilit görevlileri tanımlayın

YAZILI RAPORLAR

Yazılı raporların istihbaratın yayılmasının büyük bir bölümünü oluşturması muhtemeldir. Yazılı bir rapor, bir durumun veya analizin temel unsurlarının belirli bir hedef kitleye sunumudur. Seyirci, yalnızca en küçük bültene ihtiyaç duyan devriye memurlarından, daha ayrıntılı raporlara ihtiyaç duyan kıdemli memurlara ve her şeye ihtiyaç duyabilecek meslektaşlarına kadar değişebilir. Gelecekteki bir eylem planının temeli olabilecek bir analize genel bir bakış sunmak için kullanıldığında en etkilidir - örneğin zamanın potansiyel bir operasyonu etkileyen çok önemli bir faktör olmadığı durumlarda.

Yazılı bir raporun doğrudan geri bildirim/sorgulama için çok az fırsat yarattığını hatırlamak önemlidir.

Okunduğu zaman kendi değerini iletmeli ve kendi noktalarını koymalıdır. Sözlü bir sunumda olduğu kadar tekrar anlatma şansınız yok. Bu, yazılı raporların okuyucuyu etkilemeye başlar başlamaz profesyonelce sunulması gerektiği anlamına gelir. Akıllı, renkli, net bir brifing sayfasının, uzun, dağınık bir metin sayfasından ziyade daha etkili olması daha olasıdır.

Raporlar, hem doğruluk hem de noktaların netliği için kanıt okumalı olmalıdır, mümkünse bunu sizin için başka birine yaptırın. Bu, raporun güvenilirliğini artıracak ve doğru mesajın iletilmesini sağlamaya yardımcı olacaktır.

SONUÇLARIN SUNUMU

Koşullar , raporun hızlı ve olumsuz koşullar altında formüle edilmesi gerektiğini zorunlu kılabilir, ancak yazar, mümkün olan her yerde iyi bir sözlüğe, eş anlamlılar sözlüğüne ve yazı malzemelerine sahip olmaya çalışmalıdır.

Bir kelime işlemcinin kullanılması, rapor yazarınınverimliliğine yardımcı olacaktır.Belgeler göreli kolaylıkla oluşturulabilir, kaydedilebilir ve manipüle edilebilir.

sunmanın bir sözlü brifing vermek yerine birkaç avantajı ve dezavantajı vardır .

Avantajlar	Dezavantajları
Rapor, belirli bir alıcının ihtiyaçlarına uyacak şekilde uyarlanabilir, böylece o kişinin gereksinimleriyle alakasız ve/veya önemsiz bilgiler hariç tutulabilir.	Rapor yazarının , bir raporun içeriğini düzene sokmak için hedef kitleyi tanıması gerekir; aksi takdirde, o sırada bildikleri kadar ayrıntıyı dahil etmeleri gerekecektir.
Raporun içeriği boş zamanlarında yeniden okunabilir ve alıcı tarafından ileride kullanılmak üzere vurgulanan önemli noktalar.	Bir rapor yazıldığında, tarihi bir belge haline gelir, o anda eldeki bilgilere ilişkin durumun anlık görüntüsü olur.
Raporun içeriğine geri dönülebilir. Örnek: fikir alışverişi veya daha fazla bilgi alışverişi yaparken.	Yazar ile okuyucu arasındaki mesafe nedeniyle aralarındaki alışverişlerde kaçınılmaz bir gecikme yaşanmaktadır.
Daha fazla yayılım için kolay	Dağıtımını kontrol etmek daha az kolaydır .

sağlanan yapı , aynı zamanda, analizin yazılı raporunun hazırlanmasında da size iyi hizmet edebilir. Analist tarafından üretilen çizelgeler , ideal olarak, tek başına düşünülmemelidir. Bunlar, yer alan suç faaliyetinin anlaşılmasına yardımcı olmak üzere üretilmiştir ve bu, beş noktanın bir lütfen üzerinde bir kural olarak yapılmasına yardımcı olmalıdır .

İstihbarat raporları yazmak için beş ana kural

- Açık ve net olun. Hatalı ifadeler veya hesaplamalardaki hatalar raporların etkisini azaltacaktır.
- Kaydı kişiselleştirmek için üçüncü kişi olarak yazın
- Profesyonel jargon kullanmaktan kaçının
- Mantıklı bir düşünce, fikir ve argüman akışı sağlayın
- Doğru yazım ve dilbilgisi sağlayın. Yazım hataları okuyucunun dikkatini dağıtmakta, isim ve kimliklerde kafa karışıklığına neden olabilmektedir.

Rapor , en önemli bulguları, sonuçları ve tavsiyeleri içermelidir .
gibi , yazılı raporun da basit basit bir dilde analize sonuç vermesi ve vurgulanması gereken noktaları tanımlaması gerekir. İçerik açık, özlü, iyi yazılmalı ve uzun baskı bloklarından kaçınılarak boşluk bırakılmalıdır.

bir yapı, ters çevrilmiş piramittir . Kullanın, rapordaki her paragrafın, uçta ters duran bir piramit olduğunu hayal edin. En önemli fikir, piramidin en geniş kısmında (konu cümlesinde) olmalıdır ve o paragraftaki diğer tüm fikirler bu öncü fikri destekler. Aslında konu cümlesinden sonra gelen cümleler önem sırasına göre yerleştirilmelidir.

Benzer şekilde, tüm istihbarat raporuna ters çevrilmiş bir piramit olarak yaklaşılabilir. En önemli bilgi eserin sonunda değil başında olmalıdır. Bu ilk bölüm yeterince ilgi çekiciyse, okuyucu okumaya devam edecektir. Yazılı bir rapor hazırlarken, okuyucunun önce "büyük fikri" öğrenmek istediğini unutmayın; büyük fikir sizin çıkarımınızdır. Bazı yazarlar büyük fikri raporun sonuna kadar saklarlar, tıpkı bir hikayenin sonunu beklemek gibi "punch line" ı beklemek gibi. Analitik bir raporda durum tam tersi olmalıdır. Önce kesin noktayı belirtin ve hikayeyi takip edin—çıkarımı destekleyen ayrıntılar.

Bu ilkeyi raporun tamamına (raporun organizasyonuna, rapordaki bölümlere ve her bölümdeki paragraflara) uygulamayı hatırlarsanız, raporun yazılması ve okunması daha kolay olacaktır.

Bu yaklaşıma uygun olarak, ilk üç-dört paragrafın konu cümleleri sırayla bir araya getirilerek yönetici özeti oluşturulabilir. Tekrardan kaçınmak ve dinamik okuma elde etmek için bir miktar yeniden yazma gerekli olsa da, özet paragrafın bu şekilde yapılandırılması genellikle etkilidir.

Her konu cümlesinin yapısı da okuyucunun dikkatini çekmek için önemlidir. İki bileşeni olmalıdır - "ne?" - gerçek ve "öyleyse ne?" - bu gerçeğin sonuçları. Bu şekilde okuyucu hem neler olduğunu hem de neden önemli olduğunu öğrenir.

Taslağı bitirdikten sonra, sonucu test etmek için aşağıdaki teknik kullanılabilir. Başlık tek başına hem "ne"yi ifade ediyor mu? e n'olmuş?" tüm belgenin? Ardından aynı tekniği

yönetici özetinin konu cümlesine uygulayın. Son olarak, her paragrafın açılış cümlesi de bu gereksinimi karşılamalıdır.

Tersine çevrilmiş piramit modelinin bir yan yararı, istihbarat raporunun kısa tutulmasına yardımcı olmasıdır. Bu teknik, yazarı yalnızca konuyla doğrudan ilgili olan gerçeklere odaklanmaya zorlar. Ayrıca hangi gerçeklerin gerekli olduğunu ve hangilerinin "bilmek güzel" olduğunu belirlemeye yardımcı olur.

Son olarak, iyi yazma genellikle iyi yeniden yazma anlamına gelir. Bildirildiğine göre, Mark Twain bir keresinde bir arkadaşından uzun bir mektup gönderdiği için özür diledi, çünkü kısa bir mektup yazacak zamanı yoktu.

En yaygın üç yazım hatası

- *Büyük birikim* — yazar vakayı yavaş yavaş oluşturur ve sonuçları sona saklar. Teori, muhtemelen, bu şekilde sonuçların daha dramatik görüneceği yönünde. Ne yazık ki, çoğu okuyucu sona ulaşmadan okumayı bırakacaktır.
- *Zaman çizgisi* -yukarıdaki hataya biraz benzer olan bu yaklaşım, bir hikayeyi kronolojik sırayla anlatmayı amaçlar ve bu nedenle en önemli ve ilgili öğeleri sonuna kadar saklar. Bununla birlikte, tipik olarak, okuyucu en çok son olaylarla ilgilenir ve sabrını kaybeder.
- *Zor iş* — bu yaklaşım aynı zamanda "bak bu konuda ne kadar bilgim var" olarak da bilinir. Tipik olarak, istihbarat analistleri büyük miktarda bilgi toplar ve çoğu zaman hiçbirini dışarıda bırakmaya dayanamazlar. Sonuç, uzun ve çoğunlukla odaklanmamış bir üründür.

Yazılı bir raporun içeriği:

1. Başlıklı kapak

Başlığın yanı sıra kapak sayfasında analistin adı, birimi ve raporun yazıldığı tarih büyük olasılıkla yer alacaktır. Hemen dikkat çekecek uygun bir başlık seçin. Ayrıca belge kısıtlı ise bu belirtilmelidir.

2. İçindekiler sayfası

Bu, çoğu durumda özellikle tüm belgenin çok sayıda çizelge, ek vb. olduğu durumlarda gerekli olacaktır.

3. Önsöz/yöntem

Önsöz kısa olmalı ve yapılan analizin türü, kullanılan yöntemler, analizin amacı, analizin yapıldığı ekip ve ilgiliyse analizin kapsadığı dönemlerin ayrıntılarını içermelidir. Ek olarak, bu, metin bölümlerini vurgulamak için kullanılan herhangi bir yöntemin anahtarını ve istihbarat çizelgelerindeki varlıkları ve bağlantıları temsil etmek için kullanılan herhangi bir sembolün anahtarını içermelidir.

4. Özet veya genel bakış

Çıkarım ifadesinin genişletilmesi, raporun yönetici özeti veya genel görünümü haline gelir. Özet yine kısa olmalı ve hipotezlere ve sonuçlara, öncüllere ve tavsiyelere dayanan sonuçların bir özetini içermelidir.

5. Ana rapor

Binalar ve bunların türetildiği bilgiler, raporun ana bölümleri haline gelir. Bir kez daha bu kısa tutulmalı ve kullanılan tüm öncüllerin sonucunu belirten çıkarımla başlayan analizin yapısını mantıklı bir şekilde tanımlamalıdır. Öncüller daha sonra, raporun ana bölümlerinde rakamlar haline gelen bağlantı çizelgeleri ve finansal profiller gibi bilinen ilgili istihbarat ve küçük çizelgeler tarafından tanımlanır ve desteklenir. Her durumda metne farklı bir arka plan rengi kullanarak kutulama gibi yöntemlerle okuyucunun dikkatinin çıkarımlara ve analist yorumlarına (istihbarat boşluklarının vurgulanması gibi) çekilmesi önerilir. Fotoğraflar da bu bölüme dahil edilebilir, ancak çok fazla fotoğrafın raporun gelecekte e-posta ile yayılmasını engelleyebileceğine dikkat edilmelidir.

6. Sonuçlar/tavsiyeler

Raporun son bölümü, sonuç olarak çıkarımın/seçilen çıkarımların bir tekrarını içerebilir ve analizin sonucuna sağlam bir şekilde dayanması gereken tavsiyeler için bir liste ve rasyonel sağlayabilir.

7. İstihbarat boşlukları

Bazı istihbarat raporlarında, istihbarat boşluklarını, ilgili boşluğu doldurmak için hareket edebilecek kurum/ülkeye göre gruplandırılarak tek bir bölümde listelemek son derece yararlıdır. Bu, ilgili tarafların nelere göre hareket etme sorumluluklarını görmelerini ve raporun kullanıcılarının bu sürece ilişkin ilerlemeyi başlatmasını ve kontrol etmesini sağlar.

8. Ekler ve dizin

Bu son bölüm, raporun içeriğini grafik olarak gösteren daha büyük veya ek çizelgelerin eklenmesi içindir.

Bir tür eylem veya yanıt arıyorsanız, talebin uygulanabilir ve gerçekçi olup olmadığını değerlendirin. Makul olmayan veya imkansız talepler, gelecekteki yayınlar üzerinde zararlı bir etki ile güvenilirlik kaybına neden olur. Raporda, soruların nasıl sorulması gerektiğine veya ifadelerin nasıl açıklığa kavuşturulacağına dair bir gösterge yer almalıdır. Bu, okuyucunun yazara ulaşabileceği bir iletişim noktası sağlamayı gerektirebilir.

Herhangi bir rapor gönderilmeden önce yazar, mantıklı olduğundan, yazımın doğru olduğundan (özellikle isimler ve yerlerin), raporun okunaklı olduğundan ve içeriğin doğru olduğundan emin olmak için okumalıdır. Örnek: doğum tarihleri.

Bu, kendi başına güvenilirlik katacak ve özellikle rapor mahkemeye sunulacaksa, soruşturma sürecindeki sorunları önleyecektir.

Bu model, analistin, başka bir deyişle, analiz sonuçlarını mümkün olan en açık, en kısa ve en mantıklı şekilde ileten, amaca ulaşan bir belge oluşturmasına yardımcı olmak için bir rehber olarak tasarlanmıştır.

Yazılı veya sözlü herhangi bir sunumun yapısı ve sunumu maksimum etki yaratacak şekilde olmalıdır. Bu, yapıcısı adına hayal gücü ve özgünlük gerektirir.
Analistler bu yetenekleri pratik ve deneyimle geliştireceklerdir.

Ek I. Örnek: cezai bilgiler ve istihbarat yönergeleri

I. Suç bilgileri ve istihbarat yönergeleri

Bu yönergeler (kurum adı), suç faaliyetleriyle ilgili veritabanı için kabul edilen standartları sağlar. Bu veri tabanı, (kuruluşun istihbarat misyonunda belirtilen) "suç faaliyetine karıştığından şüphelenilen kişi ve gruplara ilişkin bilgileri toplamak, değerlendirmek, derlemek, analiz etmek ve yaymak ve bu bilgileri ilgili kişilere sağlamak" gibi (kuruluşun) misyonunu yerine getirmek için oluşturulmuştur. suç önleme ve karar verme amaçları için İcra Kurulu Başkanı").

Bu standartlar, (yetki alanı) vatandaşlarının medeni hak ve özgürlükleri ile yasa uygulayıcının suçla ilgili bilgi toplama ve suçla ilgili bilgi yayma ihtiyacı arasında adil bir denge sağlamak için tasarlanmıştır. suç faaliyeti.

II. Suç bilgileri ve istihbarat tanımlanmış

(Ajans adı) amaçları doğrultusunda, Suç Bilgi ve İstihbarat Veritabanı, aşağıdakilerin faaliyetleri ve dernekleri hakkında depolanmış bilgilerden oluşacaktır:

A. Kişiler:

1. suç eylemlerinin fiilen veya planlanması, organize edilmesi, finanse edilmesi veya işlenmesine dahil olduklarından veya olduklarından makul olarak şüpheleniliyorsa ; veya

B. Kuruluşlar, işletmeler ve gruplar:

1. suç eylemlerinin fiilen veya planlanması, organize edilmesi, finanse edilmesi veya işlenmesine dahil olduklarından veya bu eylemlere dahil olduklarından makul olarak şüpheleniliyorsa; veya
2. bilinen veya şüpheli suçlular tarafından işletildiğinden, kontrol edildiğinden, finanse edildiğinden veya sızıldığından makul olarak şüpheleniliyorsa.

III. Dosya içeriği

Cezai Bilgi ve İstihbarat Veritabanında (CIID) yalnızca (kurumun) dosya girişi kriterlerini karşılayan suçlulara ve suç eylemlerine bağlantısı olan bilgiler saklanacaktır.

Özel olarak hariç tutulan materyal, herhangi bir bireyin veya herhangi bir grubun, birliğin, şirketin, işletmenin, ortaklığın veya başka bir kuruluşun siyasi, dini veya sosyal görüşleri, dernekleri veya faaliyetleri hakkındaki bilgileri içerir, ancak bu tür bilgiler doğrudan bireyi, grubu içeren suç davranışıyla ilgili değilse , şirket veya dernek.

CIID ayrıca geçerli herhangi bir federal, Eyalet veya yerel yasa veya yönetmeliği ihlal ederek elde edilen hiçbir bilgiyi içermeyecektir.

IV. Dosya kriterleri

Suç Bilgi ve İstihbarat Veri Bankasında (CIID) tutulan tüm bilgiler (kurum adı) tarafından belirtilen dosya kriterlerini karşılamalıdır. Genel olarak bilgiler, genel kabul görmüş ceza istihbarat dosyası standartlarına uygun olarak saklanacaktır.

A. Genel dosya kriterleri

1. Bir veya daha fazla suç eyleminin planlanması, organize edilmesi, finanse edilmesi veya işlenmesine fiilen veya teşebbüste bulunduğundan veya dahil olduğundan makul olarak şüphelenilen bir kişi, kuruluş, işletme veya grupla ilgili bilgiler CIID'ye dahil edilecektir:3

a. cinayet
b. kredi paylaşımı
c. kumar
ç. narkotik dağıtımı
d. gasp
e. kundakçılık
f. kaçırma
g. çalıntı mal almak
ğ. komplo
h. Kara para aklama
ı. şantaj
i. aldatma yoluyla hırsızlık
j. sahtekar
k. kalpazanlık
l. kimlik Hırsızı
m. bombalama
n. terörizm

2. Yukarıdaki suç faaliyetlerinin bir veya daha fazlasının kapsamına girmeye ek olarak, kalıcı statü verilecek özne/kuruluş, bir ad ve benzersiz tanımlayıcı özelliklerle (örn. güvenlik numarası, yabancı kayıt numarası, ehliyet numarası, adres). Konuyu/varlığı mevcut dosya girişlerinden ve daha sonra girilebilecek olanlardan ayırt etmek için dosya girişi sırasında tanımlama gereklidir.

Not: Bu kuralın istisnası, modus operandi (MO) dosyalarını içerir. MO dosyaları, belirli bir suç senaryosu türü için benzersiz bir çalışma yöntemini tanımlar ve tanımlanabilir bir şüpheliyle hemen bağlantılı olmayabilir. Ek tanımlayıcılar aranırken MO dosyaları süresiz olarak tutulabilir. Ayrıca, suç ve terör faaliyetlerinde bulunanlar tarafından çoklu ve yanlış tanımlayıcıların yaygın olarak kullanılması nedeniyle, kişi için tutulan tanımlayıcıların doğru olabileceği veya olmayabileceği de belirtilmelidir.

[3] Veritabanı, dar bir suç faaliyetine odaklanmak üzere tasarlanıyorsa, belirtilen suç eylemleri bu odağı yansıtacaktır. Örneğin, veri tabanının odak noktası terörle mücadeleyse, gösterilen suçlar şunlar olabilir: kundakçılık; kamu görevlilerine ve özel vatandaşlara yönelik tehditler; yıldırma veya siyasi motivasyon amacıyla patlayıcı cihazların üretimi, kullanımı veya bulundurulması; kamu veya özel mülkiyetin yok edilmesi; halka zararlı biyolojik maddeler salmak; nükleer silahların yetkisiz patlatılması; başkalarını terör faaliyetlerine katılmaya teşvik etmek veya teşvik etmek; terör faaliyetlerini desteklemek için kullanılacak fonları istemek veya almak; operatörlere yönelik saldırılar veya toplu taşıma araçlarına yardım; terör silahı olarak kullanılacak araç veya malzemelerin çalınması; terörle bağlantılı bireyler veya gruplar tarafından işlenen herhangi bir suç eylemi.

B. Geçici dosya kriterleri

Kalıcı saklama kriterlerini karşılamayan ancak daha önce listelenen kategorilerden birini içeren bir soruşturmayla ilgili olabilecek bilgilere geçici statü verilmelidir. Geçici bilgiler, kalıcı hale getirilmesi için zorunlu bir sebep olmadıkça bir yıldan fazla saklanamaz. (Mücbir sebep örneği, bir suçun işlendiğine dair birden fazla bilgi bulunması, ancak bir şüphelinin kimliğinin tespit edilmesi için bir yıldan fazla bir sürenin geçmesi gerektiğidir.) Bu süre zarfında, süjenin/kişinin belirlenmesi veya doğrulanması için çaba gösterilmelidir. nihai durumunun belirlenebilmesi için bilgiler. Bir yıllık sürenin sonunda bilgi hala geçici olarak sınıflandırılıyorsa, bilgi silinmelidir. Bir bireye, kuruluşa, işletmeye veya gruba aşağıdaki durumlarda geçici statü verilebilir:

1. Özne/varlık tanımlanamaz—özne/varlık (suç faaliyetlerine karıştığından şüphelenilse de) bilinen fiziksel tanımlayıcılara, kimlik numaralarına veya ayırt edici özelliklere sahip değildir.

2. Müdahale şüphelidir—aşağıdakilerden birine sahip bir özne/kuruluş, suç faaliyetlerine karıştığından şüphelenir:

    a. Muhtemel suç örgütleri—bireysel organizasyon, işletme veya grup (şu anda suç olarak aktif olduğu bildirilmemiştir) bilinen bir suçluyla ilişki içindedir ve yasa dışı faaliyetlerde ortak olarak yer alıyor görünmektedir.

    b. Daha sonra suç faaliyetine karıştığı bilinen kişilerle ilişki geçmişi olan ve şu anda rapor edilen koşullar, suç faaliyetlerine aktif olarak dahil olabileceklerini gösteren tarihi dernekler—birey, kuruluş, işletme veya grup (şu anda suç faaliyetinde olduğu bildirilmeyen) aktivite.

V. Bilgi değerlendirmesi

Cezai Bilgi ve İstihbarat Veritabanında tutulacak bilgiler, dosyalanmadan önce güvenilirlik ve içerik geçerliliği açısından değerlendirilecek ve belirlenecektir. Bir istihbarat birimine alınan veriler, doğrulanmamış iddialardan veya bilgilerden oluşabilir. Bilginin kaynağının ve içeriğinin değerlendirilmesi, gelecekteki kullanıcılara bilginin değerini ve kullanışlılığını gösterir. Kaynak güvenilirliğinin zayıf olduğu veya içerik geçerliliğinin şüpheli olduğu durumlarda değerlendirilmemiş olabilecek bilgilerin dağıtılması, ajansın faaliyetlerine zarar verir ve bireyin mahremiyet haklarına aykırıdır. Bu değerlendirme, kaynak ve verilerin değerlendirilmesi ile ilgili Bölüm 4'te daha önce belirtildiği gibi sistematik olarak gerçekleştirilmelidir.

VI. Bilgi sınıflandırması

Suç Bilgi ve İstihbarat Veritabanında tutulan bilgiler, kaynakları, soruşturmaları ve bireyin özel hayatın gizliliği hakkını korumak amacıyla sınıflandırılır. Sınıflandırma ayrıca, bilgilerin kurum dışındaki kişilere açıklanmasından önce gerekli olan dahili onayı da gösterir.

Bilgi ve istihbaratın sınıflandırılması sürekli değişime tabidir. Zamanın geçişi, soruşturmaların sonucu ve diğer faktörler, belirli belgelere atanan güvenlik sınıflandırmasını etkileyebilir. İstihbarat dosyalarındaki belgeler, bilgilerin yalnızca uygun olduğunda ve uygun olduğunda serbest bırakılmasını sağlamak için daha yüksek veya daha az düzeyde belge güvenliğinin gerekli olup olmadığını belirlemek için sürekli olarak gözden geçirilmelidir.

A. Hassas sınıflandırma seviyesi:

1. Şu anda soruşturma altında olan önemli suç faaliyetlerine ilişkin bilgiler
2. Muhbir kimlik bilgileri

3. Sıkı dağıtım ve yayın kriterleri gerektiren istihbarat raporları

B. Gizli

1. Hassas olarak tanımlanmayan suç istihbarat raporları
2. Hassas olarak sınıflandırılmayan ve yalnızca kolluk kuvvetlerinin kullanımına yönelik istihbarat bölümü kanallarından elde edilen bilgiler.

C. Kısıtlı

1. Daha önceki bir tarihte hassas veya gizli olarak sınıflandırılan ve üst düzey güvenlik ihtiyacının artık mevcut olmadığı raporlar
2. Kolluk kuvvetleri için/onlar tarafından hazırlanan gizli olmayan bilgiler.

D. Sınıflandırılmamış

1. Orijinal haliyle genel halkın erişebildiği vatandaşlıkla ilgili bilgiler (yani kamu kayıtları)
2. Medya bilgileri (yani kamu raporları, gazeteler ve dergiler)

VII. Bilgi kaynağı belgeleri

Her durumda, kaynak kimliği mevcut olmalı ve verilerin kendisiyle birlikte not edilmelidir. Kaynağın korunması gerekmedikçe kaynağın gerçek kimliği kullanılmalıdır. Kaynağın isimle tanımlanmasının güvenlik nedeniyle pratik olmadığı durumlarda, bir kod numarası kullanılabilir. Kodlanmış bilgi kaynaklarının gizli bir listesi, istihbarat birimi süpervizörü tarafından, belki de bir gizli kaynaklar kaydının veya veri tabanının bir parçası olarak saklanmalıdır.

VIII. Bilgi kalite kontrolü

Suç Bilgileri ve İstihbarat Veritabanında saklanacak bilgiler, dosyalanmadan önce dosya yönergelerine ve kurum politikasına uygunluk açısından kapsamlı bir incelemeden geçecektir. İstihbarat birimi amiri, CIID'ye girilen tüm bilgilerin kurumun dosya kriterlerine uygun olduğunu ve uygun şekilde değerlendirilip sınıflandırıldığını görmekten sorumludur.

IX. Bilgi ve istihbarat yayma

A. Açık kamu kayıtları muafiyeti

(Ajans adı) tarafından oluşturulan, derlenen, elde edilen veya sürdürülen cezai istihbaratla ilgili tüm belgeler, materyaller ve bilgiler gizli, kamuya açık olmayan ve Bilgi Edinme Özgürlüğü Yasası (FOIA) veya diğer kamu bilgilendirme düzenlemelerine tabi değildir. veya yasalar.

B. Kriterler

CIID'den alınan bilgiler, yalnızca hem bilme ihtiyacı hem de bilme hakkını kanıtlamış bir kişiye verilebilir. "Bilme hakkı", talepte bulunanın aranan bilgiyi almak için resmi bir ehliyete ve yasal yetkiye sahip olması olarak tanımlanır. "Bilmesi gereken", talep edilen bilgilerin bir soruşturmayı başlatma, ilerletme veya tamamlama konusunda talepte bulunan kişiyle ilgili ve gerekli olması olarak tanımlanır.

C. Üçüncü taraf veri kısıtlamaları

Harici bir kuruluştan alınan hiçbir "aslı", menşe kuruluşun izni olmaksızın üçüncü bir kuruluşa verilemez.

Ç. Verilerin sınıflandırılması yoluyla bilginin yayılması

Aşağıdaki sınıflandırmalardaki bilgiler, aşağıdaki personelin onayı ile yayılabilir:

Güvenlik seviyesi	Yaygınlaştırma kriterleri	Yayın Otoritesi
Duyarlı	Belirli bir bilmesi gereken kolluk kuvvetleri personeliyle sınırlıdır ve bilme hakkı	(Yönetim Adı)
Gizli	Hassas için aynı	İstihbarat Şube Amiri
	Kısıtlı / Hassas	İstihbarat Bölüm Amiri ile aynı
sınıflandırılmamış	Sınırlı değildir	İstihbarat Şube Amiri

D. Yakın tehlikeyi önlemek için yayma

Bu yayma kısıtlamalarındaki hiçbir şey, bir istihbarat değerlendirmesinin bir hükümet yetkilisine veya gerektiğinde, can veya mal için yakın tehlikeyi önlemek için herhangi bir başka kişiye yayılmasını sınırlamaz.

E. yaygınlaştırma kontrolü

Sistemin yetkisiz kullanımını ve kötüye kullanımını ortadan kaldırmak için (ajans adı), saklanan her belgeyle birlikte muhafaza edilen bir yayma kontrol formu kullanacaktır. Bu denetim kontrolü şunları kaydeder:

1. Talep tarihi;
2. Ajansın adı;
3. Bilgileri talep eden kişi;
4. Bilmem gerek;
5. Sağlanan bilgiler;
6. Talebi işleyen çalışanın adı.

X. Dosya inceleme ve temizleme

CIID'deki bilgiler, dosyanın güncel, doğru ve (kurum adı); federal ve eyalet yasaları kapsamında güvence altına alınan bireyin mahremiyet hakkını korumak; ve güvenlik sınıflandırma seviyesinin uygun kalmasını sağlayın.

A. Temizleme kriteri

Bilgiler, aşağıdaki hususlar kullanılarak gözden geçirilecek ve/veya temizlenecektir:

1. Fayda—son iki yılda kullanıldı mı?
2. Zamanındalık ve uygunluk—soruşturma halen devam ediyor mu?
3. Doğruluk ve eksiksizlik—bilgi hala geçerli mi?

B. Zaman çizelgesini gözden geçir ve temizle

1. Kalıcı veriler—kalıcı veriler her beş yılda bir gözden geçirilecek ve/veya silinecektir 2. Geçici veriler—geçici veriler her yıl gözden geçirilecek ve/veya silinecektir.

C. İmha şekli

1. CIID'den temizlenen malzeme imha edilecektir. İmha, bir kişiyi adıyla tanımlayan tüm kayıtlar veya kağıtlar için kullanılır.

XI. Dosya güvenliği

A. Fiziksel güvenlik

CIID, dosya erişiminin yetkili personelle sınırlı olduğu güvenli bir alana yerleştirilmelidir.

B. programatik güvenlik

CIID, bilgileri izinsiz değiştirilemeyecek, yok edilemeyecek, erişilemeyecek veya temizlenemeyecek şekilde sistemde depolamalıdır. Sistemde yer alan bilgilerin yetkisiz olarak erişilmesi, kullanılması veya ifşa edilmesi durumunda yaptırımlar uygulanacaktır. Bunu başarmanın en iyi yolu, muhtemelen bir denetim izinin oluşturulması ve periyodik denetim ve teftiş incelemeleri olacaktır.

yetki

Bu Yönergeler derhal yürürlüğe girecektir.

_____

Ajans Başkanı

Ajans Adı Tarih:

Ek II. önerilerde bulunmak

Son çıkarıma varmak için en az bir kez ve muhtemelen birkaç kez istihbarat sürecinden geçen analist, araştırma veya proje hakkında derinlemesine bilgi sahibi olacaktır. Analizin müşterileri (araştırmacılar/yöneticiler) tarafından bile eşleştirilemeyecek bir bilgi düzeyi. Herhangi bir analizin nihai sonucu ileriye dönük yolu işaret etmek olmalıdır.

"Şimdi ne yapıyoruz", hatta "Ne yapmıyoruz" sorusunu ele almak için. Kaynak bulma kararları vermek değil, onları bilgilendirmek analistin rolüdür. Önerilerde bulunmak sürecin meşru bir parçasıdır, ancak önerilerin kapsamı ve ayrıntıları, analizin kime yönelik olduğuna ve sağlanan çıkarımın türüne göre değişebilir. Öneriler genel olarak aşağıdaki alanlara bölünecektir:

Daha fazla bilgi toplama/yönlendirilmiş veri toplama (istihbarat boşluklarını doldurma) - Çıkarımları test etmek için gereken özel bilgiler. Bu tavsiyeler, kaynakların alakasız bilgiler toplayarak israf edilmemesini sağlayan istihbarat sürecinin ilk aşamasına geri dönüş için odak sağlar. Analistler, bu tür bilgilerin nasıl elde edilebileceğini düşünmek ve olası alternatifler önermek isteyebilirler; ancak analizin değerini azaltabilecek açık ifadelerden kaçınmak için dikkatli olunması gerekir.

Hedef seçimi —Bir suç ağının analizinin bir sonucu olarak, analist, yetersizlikleri ağın bir bütün olarak bozulmasına neden olacak hedef statüsü için bireyleri tavsiye edebilir. Bu, özellikle pazar veya suç iş profilleri hazırlanırken uygundur.

Önleyici tedbirler — Bir kanun yaptırımı ortamında, suçluları tutuklamak ve kovuşturmak üzerine kafa yormak çok kolaydır. Bununla birlikte, suçun ilk etapta oluşmasını önlemek için kullanılabilecek başka yöntemler ve yollar vardır. Bu, analistlerin nesnelliğinin ve yanal düşüncesinin eski sorunlara yeni çözümler getirebileceği bir alandır. Bu tür tavsiyeler suç örüntüsü analizinde, sorun profillerinde ve stratejik raporlarda uygun olabilir.

Tahminler/riskler —Doğaları gereği bunlar tartışmalı olabilecek tavsiye türleridir. Bu tür tavsiyelere dayandırdığınız destekleyici faktörleri açıkça belirtme yeteneği hayati önem taşımaktadır; bu tür tavsiyeler potansiyel olarak ifşa konusu olabilir ve bu nedenle yasal incelemeye açık olabilir. Risk analizi, insan hakları mevzuatının ortaya çıkmasıyla keskin bir şekilde odaklanılan yeni bir konudur.

Politika/süreç —Özellikle stratejik analiz projeleri, tavsiyelerin konusu olabilecek mevcut politikalar, süreç veya kaynak seviyelerindeki zayıflıkları vurgulayabilir. İdeal olarak, bu tür eleştiriler, sorunu ele alan alternatif bir çözüm içermelidir.

Bu, hiçbir şekilde ayrıntılı bir liste değildir ve bu ve diğer tavsiye türleri, uygun olduğu şekilde tüm analitik ürünler yelpazesine dahil edilebilir. Bazı analizler yalnızca bir tür tavsiye gerektirebilir, diğerleri birkaç tane. Analistler, bu alanda doğal olarak ilk görevlendirmede verilen yön tarafından yönlendirilecektir. Orijinal özetin bir parçasını oluşturmayan daha önemli tavsiyeler olduğunu düşünüyorsanız, bunlar sözlü olarak veya ana raporun ayrı bir eki olarak sunulabilir. Her iki durumda da, daha geniş bir yayından önce bunları müşteriyle tartışmanız tavsiye edilir.

Analistin tavsiyelerde bulunma yeteneği, belirli bir organizasyondaki deneyimleri ile gelişecektir. Bu deneyimin bir kısmı, kuruluşun bilgisayar erişimi, gözetim, diğer kurumlarla bağlantılar, mali soruşturmalar vb. gibi bilgi toplama yeteneği hakkında bilgi oluşturmayı içermelidir. Bu tür bilgiler, tavsiyelerin hem pratik hem de uygulanabilir olmasını sağlayacak ve böylece onları daha iyi hale getirecektir. kabul edilmesi ve benimsenmesi muhtemeldir.

Öneriler, analistin analiz aşamasında edindiği bilgileri, bir araştırmayı veya projeyi ilerletebilecek fikirlere ve çözümlere dönüştürdüğü yerdir. Bunlar, yayılmadan önceki istihbarat sürecinin temel ve son kısmıdır. Yayılan

istihbarat, analizin yargılanacağı üründür. Bu nedenle, önerilerin hazırlanmasında ve sunulmasında her türlü özen gösterilmelidir.

Ek III. Suç istihbaratı veri tabanı

I. Suç İstihbarat Veritabanı açıklaması

A. Amaç

(Ajans adı) Suç İstihbarat Veritabanı (CID), (istihbarat veritabanına sahip olmanıza neden olan yasaları veya politikaları alıntılayın) görevini yerine getirmek için oluşturulmuştur.

Bu veri tabanı, (kuruluş) suçlu bireyler ve (yargı yetkisi) içindeki ve dışındaki (yargı yetkisi) faaliyetler arasındaki bağlantıları, faaliyetin veya bireyin (yetki alanı) ile bağlantıları varsa, belirleme yeteneği sağlar. Ayrıca (kuruluşa), (yetki alanı) genelinde kanun uygulama çabalarını koordine etmek için gerekli verileri sağlar. Merkezi bilgi toplama, bu verilerin anında analiz edilmesini sağlayarak Eyalet, yerel ve federal kanun uygulayıcılarına uyarılar ve uyarılar sağlar. Ayrıca (yargı yetkisinin) bilgi paylaşım ağlarına katılmasına izin verir.

(Ajans adı) sistem politikaları, kolluk kuvvetleri içinde çok yargılı bilgi paylaşımı için standartlar sağlayan 28 CFR 23*'e dayanmaktadır.

B. Tanımlar

1. "Kullanıcı", CID sistemine katılan bir kolluk kuvvetidir.
2. "Erişim görevlisi", CID sisteminde erişim görevlisi olma kriterlerini karşılayan bir kişidir.
3. "Ajans" (ajans adı).

II. Suç İstihbarat Veritabanına Erişim

A. Erişim Kriterleri

(Ajans) tarafından belirlenen kolluk kuvvetleri CID'ye erişebilecektir.

Erişimleri şunlara bağlı olacaktır:

1. Kullanıcı ve (ajans) arasında bir Mutabakat Zaptı imzalanması.
2. En az bir kullanıcı personeli tarafından istihbarat ve sistem yönergeleri eğitiminin başarıyla tamamlanması.
3. Kullanıcı için istihbarat koordinatörü olarak en az bir kişinin atanması.
4. Onaylanmış Bilgi ve İstihbarat Yönergelerine ve bu prosedürlere sürekli uyum.

III. Erişim için protokoller

A. Kullanıcı erişim süreci

1. Erişim için nitelikli potansiyel kullanıcılar (ajans) tarafından bilgilendirilecektir.

* Bakınız http://28cfr23.org

2. Bu potansiyel kullanıcılara aşağıdakileri içeren bir paket gönderilecektir:
    a. Bir mutabakat muhtırası,
    b. Bilgi ve İstihbarat Yönergelerinin bir kopyası ve
    c. Suç İstihbarat Veritabanı protokollerinin bir kopyası
3. Erişim izni almak isteyen potansiyel kullanıcılar, birincil irtibat kişisinin kim olacağını belirten bir notla birlikte Mutabakat Zaptı'nı geri gönderecektir.

B. Erişim sonlandırma hükümleri

1. Kullanıcı sonlandırma kriterleri
    a. Kullanıcının bir çalışanının neden olduğu CID sistemindeki herhangi bir güvenlik ihlali veya
    b. Kullanıcının yetersiz güvenliğinin neden olduğu CID sistemindeki herhangi bir güvenlik ihlali veya
    c. Kullanıcı tarafından, cezai soruşturmaların yürütülmesini veya cezai bilgilerin ele alınmasını düzenleyen federal, eyalet veya yerel yasa veya yönetmeliklerin ihlali.
2. fesih süreci
    a. (Ajans başkanı) veya bir atanan, CID sistem amiri tarafından ihlal konusunda bilgilendirilir
    b. Gerekirse, (ajans başkanı) veya bir görevlendirilen, sistem denetçisine, daha nihai eylemin belirlenmesine kadar sisteme herhangi bir erişimi geçici olarak askıya almasını emredebilir. Bu, sürekli erişimin sistemin bütünlüğüne zarar verebileceği durumlarda yapılır.
    c. Sistem sorumlusu, ihlalle ilgili tüm bilgilerin toplanmasına neden olur.
    ç. (Ajans başkanı) veya bir görevli, bilgileri gözden geçirir ve ihlali gerçekleştirdiği iddia edilen Kullanıcıyı, kullanıcının suçlamalara yanıtını sunmak için bir toplantıya davet eder.
    d. Kullanıcı tarafı dinlendikten sonra, (ajans başkanı) veya bir yetkili, erişimin kalıcı olarak sonlandırılıp sonlandırılmaması gerektiğine karar verir.
    e. Kullanıcı, CID sistemi aracılığıyla veya CID sistemi için alınan tüm kılavuzları, günlükleri, güncellemeleri ve verileri sistem yöneticisine iade etmelidir.

C. Bir erişim görevlileri

3. Erişim görevlileri için kriterler
    a. Yalnızca kolluk kuvvetleri tarafından istihdam edilen kişiler erişim görevlisi olarak atanmaya hak kazanır.
    b. Yalnızca, kolluk kuvvetleri görevlerini yerine getirirken bilgileri bilmesi gereken ve verileri bilme hakkı olan kişiler erişebilir.
    c. Yalnızca gerekli CID eğitimini tamamlayan kişiler erişebilir.
4. Erişim eğitimi
    a. Kullanıcıya sisteme kabul edildiğini bildirdikten sonra, Kullanıcı erişim yetkililerini belirleyecektir.
    b. Erişim görevlileri, eğitimlerini planlamak için CID sistem süpervizörü tarafından iletişime geçilecektir.
    c. Erişim görevlileri daha sonra CID eğitimine katılır.

ç. Sistem sorumlusu, eğitimde her erişim görevlisine bir şifre, kullanım kılavuzları ve diğer gerekli materyalleri verir.

5. Erişim sonlandırma hükümleri

a. Erişimin kişisel olarak sonlandırılmasını gerektiren olaylar

i. Bir erişim görevlisinin yaşıyla birlikte işine son verilmesi ii. Bir erişim görevlisinin kullanıcı ajansı içindeki başka bir işleve devredilmesi iii. Sistem güvenliğinin kişisel ihlali iv. Kullanıcı sözleşmesinin ihlali b. fesih için süreç

i. Gönüllü

- Kullanıcı ajansı, erişim görevlisinin devri veya feshi konusunda CID sistem süpervizörünü bilgilendirir. - CID süpervizörü, o memurun erişimine izin veren şifreyi siler - Memur, CID ile ilgili tüm materyalleri (ajans adı) adresine iade eder. ii. İstemsiz
- Kişisel bir güvenlik ihlali, kullanıcı veya bir erişim görevlisini içeren CID tarafından ortaya çıkar.
- Erişim görevlisinin erişimi, sistem sorumlusu tarafından derhal sonlandırılır.
- Memur hakkında suç duyurusunda bulunulabilir.
- Kullanıcı ajansı için fesih prosedürlerine ilişkin bir soruşturma başlatılabilir. - Erişim görevlisi tüm CID materyallerini (ajans adı) adresine iade eder.

D. (Ajans adı) personeli tarafından erişim

1. CID analistleri—sistem çalışanları olarak görevlerini yerine getirmek için gerekli tüm programlara, donanıma ve verilere erişeceklerdir. Bu erişim, sorgulayıcılara yardımcı olmak ve özel olarak atanmış analitik ürünler veya projeler için eğilimleri, kalıpları ve ortak noktaları analiz etmek içindir.
2. (Ajans adı) araştırmacıları—kullanıcı ajanslarının çalışanlarına benzer bir şekilde erişim görevlisi olabilirler. Böylelikle ana indeks ve sorgulama dosyalarına giriş ve sorgulama erişimleri olacaktır.
3. Tüm (kurum adı) personelinin sistemden aldıkları bilgileri en sıkı gizlilik içinde tutmaları ve erişimlerini, aksi takdirde bu verilere erişimi olmayacak kişiler için veri elde etmek için kullanmamaları gerekmektedir.
4. Bir çalışanın sistem güvenliğine ilişkin herhangi bir ihlali derhal işten çıkarılma sebebi olabilir.

E. Erişim kısıtlamaları

1. Girişler ve sorgulamalar—erişim görevlileri veri tabanına giriş yapabilir ve sorgulayabilir.
2. Hassasiyet seviyeleri:
   a. Hassas bilgi. Bu bilgi, CID'deki en hassas verilerdir ve çok kısıtlı durumlar dışında dağıtılmayacaktır.
   b. Kesin bilgi. Bu veriler, hassas verilerden daha az kısıtlanmıştır. Sorgulayıcılara sağlanmayacak veya bir kullanıcının verileri gönderdiği söylenmeyecek. Gönderen kullanıcıyla bunun yerine iletişime geçilecek ve konuyla ilgili kimin soru sorduğu bildirilecektir. Gönderen kullanıcı daha sonra, kendi takdirine bağlı olarak, soran kullanıcıyla iletişim kurabilir ve verileri paylaşabilir.

c. Ek bilgiye ihtiyaç duyulursa, takip için kullanıcı adının gönderilmesiyle birlikte, sorgulayıcılara sınırlı hassasiyet bilgileri verilecektir.

ç. Kamu kayıtlarından veya medyadan alınan sınıflandırılmamış bilgiler, sorgulayıcılara kısıtlama olmaksızın dağıtılacaktır.

F. Erişim bildirimleri ve doğrulamalar

1. CID sistem süpervizörü, aylık giriş günlüklerinin ve sorguların oluşturulmasına neden olacaktır.
2. Bir dosyadaki bir konuyla ilgili tüm sorgulamalar, orijinal gönderen Kullanıcının soruşturma hakkında bilgilendirilmesiyle sonuçlanacaktır.
3. Kısıtlanmamış bir sınıflandırmanın tek bir konusuna birden fazla giriş yapılması, giren tüm kullanıcıların diğer girişlerden haberdar edilmesine neden olacaktır.
4. Kısıtlı bir sınıflandırma girişi içeren tek bir konuda birden fazla giriş, yalnızca genel (sınırlı olmayan) girişlerin uygun kullanıcılara bildirilmesine neden olacaktır.
5. CID sistem süpervizörü, sorgular ve girişler arasındaki tüm eşleşme olaylarını gösteren bilgisayarlı bir günlüğün tutulmasına neden olacaktır. Bu log, sorgulanan tüm kayıtların logları ile karşılaştırıldığında, sistemin "isabet oranını" gösterecektir.

IV. Fiziksel güvenlik

A. (ajans adı)

1. Müşteri Kimliğinin Konumu—Müşteri Kimliği bilgisayarı, (ajans adı) adresindeki İstihbarat Merkezi içinde güvenli bir ortamda bulunacaktır. Burası güvenli, devriye gezen bir binanın parçası.

2. İstihbarat Merkezi, bina içinde erişimin yetkili CID personeli ve yerinde olması gerektiği kanıtlanabilir diğer kişilerle sınırlı olduğu güvenli bir bölümdür.

B. Kullanıcı konumlarında

1. CID dosyalarına erişim yalnızca erişim görevlileriyle sınırlıdır.
2. Kullanıcılar, CID'ye erişim sağlayan terminali, halka açık olmayan güvenli bir yerde bulundurmalıdır.

V. Ana dizin

A. Giriş kriterleri

1. Bir konuya giriş, ancak deneğin son üç (3) yıl içinde terörist veya suç faaliyetine karıştığından makul ölçüde şüpheleniliyorsa yapılabilir.

a. T hata faaliyeti, federal veya eyalet yasaları tarafından terör eylemi olarak kabul edilen herhangi bir faaliyetin finansmanı, desteklenmesi, katılımı, taşınması veya geliştirilmesi olarak tanımlanır. Bu tür eylemler şunları içerebilir:

i. Kamu görevlilerine ve özel vatandaşlara yönelik tehditler
ii. Kundakçılık
iii. Gözdağı verme veya siyasi motivasyon amacıyla patlayıcı cihazların üretimi, kullanımı veya bulundurulması

iv. Kamu veya özel mülkiyetin tahrip edilmesi v. Zararlı biyolojik maddelerin salınması vi. Nükleer silahların izinsiz patlatılması

vii. Başkalarını terör faaliyetlerine katılmaya teşvik etmek veya teşvik etmek viii. Terör faaliyetlerini desteklemek için kullanılacak fonların talep edilmesi veya alınması ix. Toplu taşıma araçlarında operatörlere veya yardımcılara yönelik saldırılar

x. Terörist silah olarak kullanılacak araç veya malzemelerin çalınması xi. Terörle bağlantılı kişi veya gruplar tarafından işlenen herhangi bir suç eylemi

b. Suç faaliyeti, federal veya Eyalet hukukunda suç olarak sayılan herhangi bir fiil olarak tanımlanır.

c. Eğitimli bir kolluk kuvvetine veya ceza soruşturma kurumu memuruna, soruşturmacıya veya analiste bir bireyin veya örgütün tanımlanabilir bir terörist veya suça karıştığına dair makul bir olasılık olduğuna inanmak için yeterli gerçekleri ortaya koyan bilgiler mevcut olduğunda makul şüphe mevcuttur. faaliyet veya girişim.

2. Terör eylemlerinin planlanması, organize edilmesi, finanse edilmesi veya işlenmesine fiilen dahil olduğundan veya teşebbüs edildiğinden veya terörle ilgili suç faaliyetlerine karıştığından veya bu faaliyetlere karıştığından şüphelenilen kişiler, kuruluşlar, işletmeler veya gruplar hakkında girişler yapılır. davranır.

3. Herhangi bir bireyin veya herhangi bir grubun, birliğin, şirketin, işletmenin, ortaklığın veya diğer kuruluşun siyasi, dini veya sosyal görüşleri, dernekleri veya faaliyetleri hakkında, bu tür bilgiler doğrudan terörist veya suç eylemi veya faaliyeti ile ilgili olmadıkça ve hiçbir bilgi girilemez ve Bilginin konusunun terörist veya suç teşkil eden bir eyleme karıştığına veya dahil olabileceğine dair makul şüphe varsa.

4. Geçerli herhangi bir federal, Eyalet veya yerel yasa veya yönetmeliği ihlal ederek elde edilen hiçbir bilgi dahil edilmeyecektir.

B. Kalıcı statü kriterleri

1. Kalıcı statü verilecek bir özne/kişinin kimliği belirlenebilir olmalıdır - bir ad ve benzersiz tanımlayıcı özellik (örneğin, doğum tarihi, adli kimlik numarası, sosyal güvenlik numarası, yabancı kayıt numarası, ehliyet numarası, adres) ile ayırt edilmelidir.

2. Belirli bir suç senaryosu türü için benzersiz bir operasyon yöntemini tanımlayan modus operandi dosyaları, tanımlanabilir bir şüpheliyle anında bağlantı olmamasına bakılmaksızın kalıcı statüye dahil edilebilir.

3. Endekse yapılan tüm girişler, CID'ye girilmeden önce politikalara ve kriterlere uygunluk açısından gözden geçirilmelidir; bu inceleme (ajans adı) bir analist veya araştırmacı tarafından tamamlanacaktır.

4. Tüm girişler, böyle bir inceleme tamamlanana kadar bir ara dosyada tutulacaktır; bu sırada CID'ye girileceklerdir.

C. Sorular

1. Soruşturma ancak deneğin terör veya suç faaliyetine karıştığından makul olarak şüpheleniliyorsa yapılabilir.

2. Bir konu hakkında soruşturma, ancak, araştırmacının konuyu içeren bir soruşturma, kovuşturma veya analize dahil olması durumunda yapılabilir. Bu iddiayı kanıtlamak için bir vaka veya proje numarası sağlanmalıdır.

D. Geçici statü kriterleri

1. Hakkında soruşturma yapılan bir özne/varlığa geçici dosya statüsü verilebilir.
2. Bir özne/varlık yakın gelecekte tanımlanamazsa, bilinen hiçbir fiziksel tanımlayıcıya, kimlik numarasına veya ayırt edici özelliklere sahip olmadığında, ona geçici dosya statüsü verilebilir.
3. Terörist veya suç faaliyetleriyle bağlantısı şüpheli olduğunda, özneye/kişiye geçici dosya statüsü verilebilir. Bu, aşağıdakiler yoluyla gerçekleşebilir:
    a. Muhtemel terör örgütleri—birey, organizasyon, işletme veya grup (şu anda aktif olduğu bildirilmemiştir) bilinen bir teröristle ilişki içindedir ve yasadışı faaliyetlere ortak olarak katılmış görünmektedir.
    b. Daha sonra terör faaliyetlerine karıştığı bilinen kişilerle ilişki geçmişi olan ve şu anda rapor edilen koşullar, terörizme aktif olarak dahil olabileceklerini gösteren tarihi dernekler—birey, kuruluş, işletme veya grup (şu anda aktif olduğu bildirilmemiştir).

VI. yaygınlaştırma

A. (Ajans adı) istihbarat bilgilerini yalnızca bilgi alma, bakım, güvenlik ve yayma ile ilgili kabul edilen prosedürleri kabul eden kolluk kuvvetlerine yayacaktır.

B. Yayma, yalnızca bir kolluk kuvveti faaliyetinin ifası sırasında bilgiyi bilmeye ihtiyaç duyulduğunda ve bilgiyi bilme hakkının bulunduğu durumlarda gerçekleşir.

C. Bu bölümün A paragrafına bakılmaksızın, (kurum adı), can veya mal için yakın bir tehlikeyi önlemek için gerektiğinde bir devlet görevlisine veya başka herhangi bir bireye istihbarat bilgilerinin bir değerlendirmesini yayabilir.

VII. Malzemelerin güncellenmesi veya temizlenmesi

A. Sistemde tutulan ancak belirli bir süre (aşağıda gösterilmektedir) gözden geçirilmeyen herhangi bir bilgi, kullanılmadan veya dağıtılmadan önce gözden geçirilmeli ve doğrulanmalıdır.

B. Girdileri

1 Tüm girişler, eskime veya yanlışlık nedeniyle verilerin güncellenmesine ve olası tasfiyesine izin vermek için belirli programlarda gözden geçirilecektir. Aşağıdaki çizelgeler kullanılacaktır:

a. Şu anda inceleme altında olan girilen konular her iki yılda bir güncellenecek veya temizlenecektir.
b. Son zamanlarda terörist veya suç faaliyetine katılmak için girilen denekler her beş yılda bir güncellenecek veya temizlenecektir.
c. Güncelleme veya temizleme için planlanan girişler, CID veri bankası tarafından işaretlenecektir. Gönderen Kullanıcının daha sonra girişi gözden geçirmesi, güncellemesi veya dosyalardan temizlemesi istenecektir.

C. Sorular

1. Tüm sorular, gönderildikten 180 gün sonra (ajans adı) personeli tarafından otomatik olarak incelenecektir.

a. Konuyla ilgili başka bir soruşturma veya başka bir bilgi ortaya çıkmadıysa; sistem sorguyu otomatik olarak temizleyecek ve sorguyu yapana eylem hakkında bilgi verecektir.

b. Konuyla ilgili başka soruşturmalar gelirse, bilgiler son soruşturmadan sonra 180 gün boyunca saklanacaktır.
c. Sorgulama CID veri tabanındaki bir konuda ise, o konu silinene kadar sorgu dosyalarda kalır.

VIII. Yaptırımlar

Bir kolluk kuvveti bilgi sisteminin operasyonlarını kapsayan kanun ve yönetmeliklerde özel yaptırımlar mevcuttur.

A. (Dosyalar için geçerli yasalar).

IX. İzleme ve denetleme

A. Sistem katılımını ve bütünlüğünü sağlamak için (ajans adı), tüm Kullanıcıların sisteme katılımını izleyecek ve/veya denetleyecektir.

B. Otomatik izleme

1. CID, veritabanının her erişiminde yerleşik bir otomatik denetim izine sahiptir.
2. Bir erişim görevlisinin her eylemi, hangi verilere erişildiğini, bunlara kimin eriştiğini ve erişim tarihi ve saatini içeren bir günlüğe kaydedilecektir.

C. Kullanıcı konumu site ziyaretleri

1. En az iki yılda bir, her uzak site, CID erişimi ve sistem aracılığıyla alınan bilgiler için yeterli güvenlik olduğundan emin olmak için ziyaret edilecektir. 2. Bu ziyaretler (ajans adı) personeli tarafından tamamlanacaktır.

X. Afet hazırlığı

A. Sistem amiri, asgari olarak aşağıdaki unsurları içeren belgelenmiş bir afet planının oluşturulmasını sağlayacaktır:

1. Sistem arızası durumunda kullanılacak CID iş yükünü işlemek için yeterli kapasiteye sahip alternatif bir bilgisayar sahasının belirlenmesi.
2. Yedeklemenin site dışı depolanmasıyla veritabanı içeriğinin haftalık yedeklemesi.
3. Gerektiğinde alternatif sahada operasyonları başlatmak ve sürdürmek için izlenecek prosedürler.

B. Afet müdahale testi

1. Sistem süpervizörü, felaket kurtarmanın uygulanabilirliğini sağlamak için tüm felaket müdahale unsurlarının yıllık olarak test edilmesini sağlayacaktır.
2. Bu testin bir raporu (ajans başkanına) veya atanan kişiye verilecektir.
3. Bildirim—(Ajans başkanı) veya atanan kişi, herhangi bir gerçek bilgisayar felaketinden hemen haberdar edilecektir.

XI. Protokollerdeki değişiklikler

A. Bu kılavuzdaki tüm protokoller (ajans başkanı) tarafından kabul edilmiş ve oluşturulmuştur.

B. Bu protokollerde yapılacak herhangi bir değişiklik (ajans başkanı) veya atanan kişi tarafından onaylanmalıdır. Bu protokollere dayalı olarak oluşturulan herhangi bir rutin, CID sistem süpervizörünün sorumluluğu altında değiştirilebilir.

Referanslar

1. Suç İstihbarat Analizi (Batı Yorkshire Polisi, 1998).
2. 2003 Anacapa Bilimleri A.Ş.
3. B. Fiora, "Okunan Istihbarat Raporları Yazmak" (*Rekabetçi Istihbarat Dergisi* , cilt 5 Sayı 1 Ocak-Şubat 2002).
4. D. McDowell "Stratejik Istihbarat" (Istana Enterprises, 1998).
5. Europol Analitik Birimi, Lahey 10-21 Mayıs 1999.
6. Europol İstihbarat Yönergeleri.
7. IACP Kriminal İstihbarat Paylaşımı Zirvesi Katılımcı Materyalleri, bölüm 3.
8. IACP, Suç İstihbarat Paylaşımı: Yerel, Eyalet ve Federal Düzeylerde İstihbarat Liderliğinde Polislik için Ulusal Bir Plan. Ağustos 2002.
9. ICPO-Interpol Suç İstihbarat Analizi Yönergeleri (Vers. 3, 2000).
10. Intelligence 2000: Temel Öğelerin Gözden Geçirilmesi, LEIU ve IALEIA, 2000.
11. M. Peterson "Criminal İstihbarat Analizinde Uygulamalar" (Praeger, 1994).
12. M. Peterson "Tartışmaya Katılmak: Ürüne Karşı Süreç (*IALEIA Journal* , cilt 11, No. 1).
13. Milli Kriminal İstihbarat Teşkilatı, Milli İstihbarat Modeli.
14. P . Andrews "Ağ Analizi Prensipleri" (Yasa Uygulayıcılarını İlgilendiren Konular: İstihbarat— En Nihai Yönetim Aracı, Kolluk Kuvvetleri İstihbarat Birimi, 1982).
15. R . Davis "Sosyal Ağ Analizi: Komplo Soruşturmalarına Yardım" (FBI Yasa Uygulama Bülteni, Aralık 1981).
16. R . Morehouse "Kolluk Uygulamasında Ceza İstihbaratının Rolü" ("İstihbarat 2000: Temel Unsurların Gözden Geçirilmesi, LEIU—IALEIA, 2000).
17. UNDCP İstihbarat Politikası ve Eğitim El Kitabı (2000).
18. Wantanabe, Frank (tarihsiz) "İstihbarat Analistleri için On Beş Aksiyom" (www.cia.gov/csi/studies/97unclass/axioms.html).
19. Batı Yorkshire Polisi Haziran 2002 ve Anacapa Yaşam Bilimleri A.Ş. 1993.
20. Beyaz Saray Görev Gücü, 2000.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

Birleşmiş Milletler yayını Avusturya'da basılmıştır

1058435 V.10-58435—Nisan 2011—100