INTERPOL

INTERPOL Kolluk Kuvvetlerini Uyarıyor: METAVERSE (SANAL EVREN) Suç Soruşturması Yöntemlerini Değiştirecek

Vaka, Suç, Adli Bilişim ve Yönetişim

Bilgilendirici Belge

Ocak 2024

İÇİNDEKİLER

Hazırlayan*:

Mehmet ŞEN, *Emekli Emniyet Müdürü, Siber Güvenlik ve Olay Yeri İnceleme Uzmanı*

Caner AKYÜREK, *Emniyet Müdürü, Finansal Suçlar ve Kripto Para Soruşturması Uzmanı*

** İnterpol'ün 18.01.2024 tarihli 'Metaverse: A Law Enforcement Perspective' isimli analiz raporunun tercümesiyle hazırlanmıştır. https://www.interpol.int/en/News-and-Events/News/2024/Grooming-radicalization-and-cyber-attacks-INTERPOL-warns-of-Metacrime*

BÖLÜM I

KOLLUK TARAFINDAN VERİLEN HİZMETLERİN VE İHBARLARIN METAVERSE ORTAMINDA YAPILMASI

Kolluk birimleri Metaverse'de sanal bir birim oluşturarak vatandaşların suçları bildirme, şikayette bulunma ve hatta sanal topluluk toplantılarına ev sahipliği yapma gibi hizmetler sunabilir. Bu sanal yaklaşım, özellikle hareket etme sorunları yaşayanlar veya uzak bölgelerde yaşayan topluluklar için polis hizmetlerini daha erişilebilir hale getirebilir. Bu aynı zamanda, özellikle kullanıcıların ve mülklerinin korunmasına yönelik farkındalık yaratma ve tavsiyeler gerektiren konularda toplumun sanal alanları kullanma konusunda daha rahat olan kesimlerine erişimi kolaylaştıracaktır. Ayrıca, kolluk kuvvetleri ile halk arasında açık iletişim için Metaverse'de topluluk alanlarının oluşturulması, daha iyi etkileşimleri ve güveni teşvik edecektir.

Source: Lexica.com

METAVERSE'DE OLAY YERİNİN KORUNMASI VE ADLİ ANALİZLERDE KULLANIMI

Kolluk kuvvetleri, fiziksel alanlar değiştirildikten çok sonra bile erişilebilen ve analiz edilebilen olay yerlerinin sanal kopyalarını oluşturmak için Metaverse'den yararlanabilir. Bu uygulama, yalnızca olay yerinin bulunduğu haliyle korunmasına yardımcı olmakla kalmıyor, aynı zamanda delillerin kapsamlı bir şekilde çapraz incelenmesine olanak tanıyarak personelin sahaya daha iyi hazırlanmasını sağlıyor. Ayrıca hakim, savcı, avukat ve mahkemeye, davanın içeriğini ve ayrıntılarını daha iyi anlamak için olay yerlerini sanal olarak ziyaret edebilme imkanı tanıyor ve bu da potansiyel olarak dava üzerinde daha fazla istişareye yol açabilir.

Source: The Times of India

BÖLÜM II

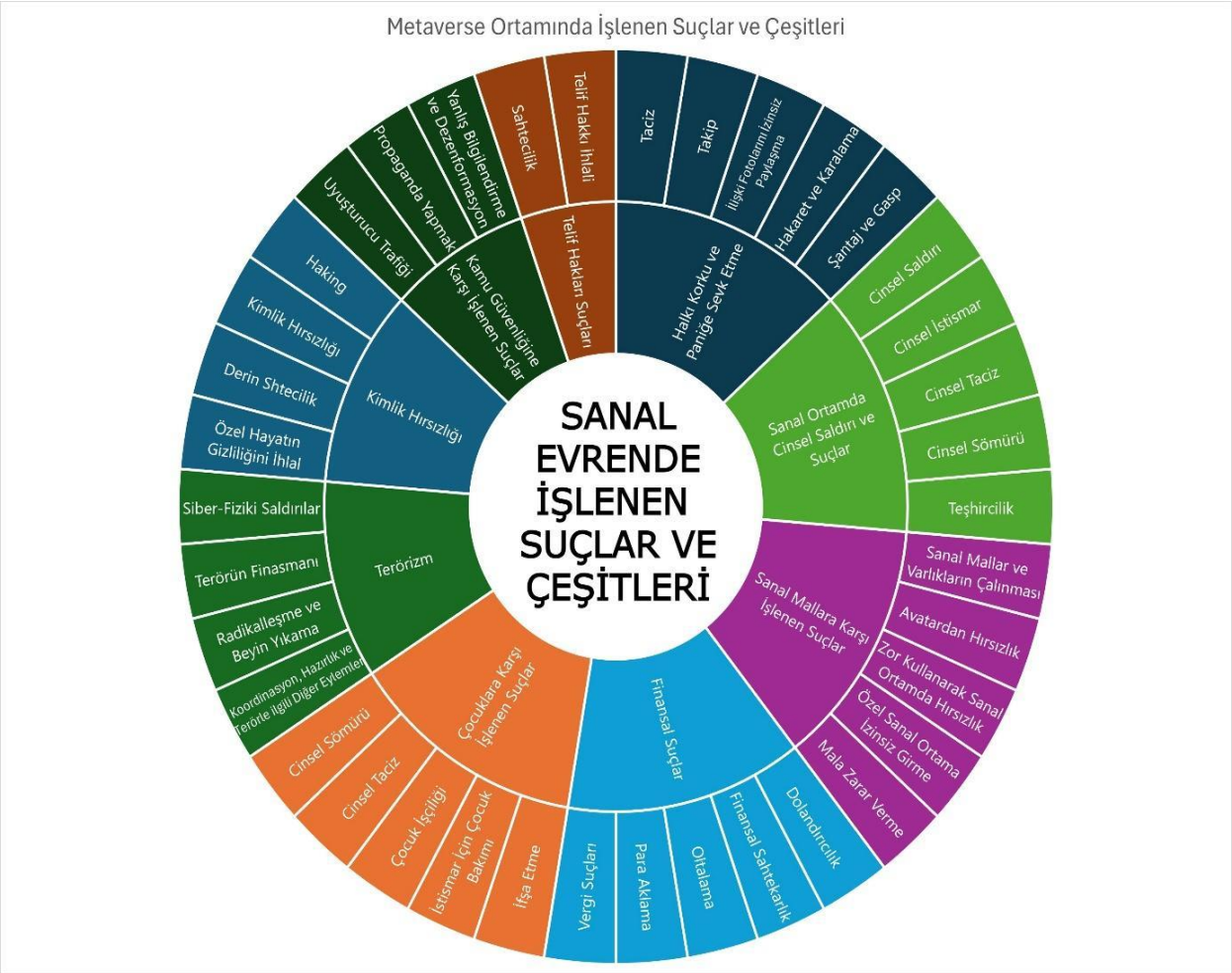
META SUÇLAR

Kullanımının ve katılımcı sayısının artmasıyla birlikte Metaverse'de nelerin suç ve zararlı olduğunun tanımlanmasına ihtiyaç duyulmaktadır. Etkili polislik ve kolluk kuvvetlerinin müdahalesi açık mevzuata bağlı olduğundan, suçların tanımlanması ve zararlı eylemlerin suç sayılması Metaverse'nin güvenliğini ve emniyetini sağlamak için gereklidir. Geçtiğimiz yıl Metaverse'deki mevcut ve potansiyel suç faaliyetlerini listelemeye çalışan birkaç rapor yayınlandı. Listede NFT dolandırıcılıkları, siber-fiziksel saldırılar, dijital kimlik hırsızlığı yoluyla kimliğe bürünme, 3D mülklerin ve sanal varlıkların çalınması, çocukların istismarı için güven ve duygusal tesis etmek, ısrarla takip ve sanal cinsel taciz gibi suçlar yer alıyordu.

Bu sektör perspektiflerine ek olarak INTERPOL, üye ülkelerdeki bazı kolluk kuvvetlerinin, özellikle mali suçlarla ilgili olmak üzere Metaverse'i içeren suçlara ilişkin raporları zaten aldığını doğruladı. Popülaritesinin artmasıyla birlikte, suç listesi daha da genişleyecek ve ortaya çıkan bu suç faaliyetlerine müdahale etmek için polis teşkilatlarını zorlayacaktır. Gerçekten de Metaverse, suçlulara "Meta suç" olarak adlandırılabilecek yeni suç türlerini işleme fırsatlarının önünü açmıştır. Meta suç giderek artan bir endişe kaynağı ve sürükleyici dünya günlük hayatımızın bir parçası haline geldikçe büyük bir sorun haline gelebilir. Bu bağlamda kolluk kuvvetlerinin çeşitli potansiyel tehditleri listeleyerek ve bunları suç sayacak yasal çerçevelerdeki boşluk alanlarını belirleyerek ortaya çıkabilecek zorlukları öngörmesi esastır.

Metaverse’deki Suçların Tipolojisi

Mevcut suç ve zarar sınıflandırmalarının güncellenmesi ve uyumlu hale getirilmesi amacıyla aşağıdaki diyagram, Metaverse'de ortaya çıkan bazı suçların ve potansiyel zararların bir tipolojisini göstermektedir. Bu meta suçlardan bazıları gerçek dünyaya kadar uzanabilir. Dünya Ekonomik Forumu, Metaverse'deki zararların tıpkı fiziksel dünyada olduğu gibi yerel veya kültüre özgü olabileceğini vurgulamaktadır. Buna ek olarak, Metaverse, özel bir yaklaşım gerektirecek jestler, duruşlar, dijital varlıklar gibi mekansal zararları da ekleyecektir.



Suç Senaryoları

Meta suç' a ilişkin daha fazla bilgi edinmek amacıyla aşağıdaki tablo, bu suçlara ilişkin spesifik işleyiş senaryolarını sunmaktadır. Sanal Evrenin karmaşık bir ortam olduğunu ve bu senaryoların hızla gelişebileceğini bilmek önemlidir. Suç aktörlerinin Sanal Evrende çeşitli suç türlerine girişebileceği çok sayıda başka yol da mevcuttur; mevcut, yeni ortaya çıkan ve tamamen yeni türler.

Suç Tipi		***Senaryo***
Kimlik Hırsızlığı	**Hackleme**	*Suçlular, bilgisayar korsanlığı veya kimlik hırsızlığı yoluyla kullanıcının hesabına ve dijital ortama yetkisiz erişim sağlayabilir. Ayrıca dijital parmak izleri de dahil olmak üzere başkalarının kimliğini çalabilir, çoğaltabilir ve satabilirler. Sahte avatarlar çalındıktan sonra suç işlemek için kullanılabilir. Buna ek olarak, sahte token ihracı, token hırsızlığı ve dolandırıcılık amacıyla token geçitleme sisteminin*
	Kimlik Hırsızlığı	

		kötüye kullanılması da dahil olmak üzere token geçişi ile ilgili riskler mevcuttur.
	Derin Sahtecilik	*Suçlular derin sahtecilik teknolojisini kullanarak çeşitli yasadışı işlemlerde bulunmak için diğer kullanıcıların kimliğine bürünebilirler. Kuruluşlar ve bireyler hakkında propaganda ve sahte haber yaymanın yanı sıra yanlış veriler yayarak bilgi ve grafik materyallerin bütünlüğünü zayıflatabilirler. Tehdit aktörleri aynı zamanda derin sahtecilik ile cinsel içerik de üretebilir iftira amaçlı istismar malzemesini yayabilirler.*
	Özel Hayatın Gizliliğini İhlal	*Suçlular kişilerin hareketleri, faaliyetleri, ilgi alanları ve kişisel bilgilerini takip ederek kullanıcının çevrimiçi gizliliğini ihlal edebilir.* *Bunlar siber zorbalıkta ve taciz için kullanılabilir.*
Finansal Suçlar	**Finansal Dolandırıcılık**	*Bilgisayar korsanlığı, sosyal mühendislik, sanal kimlik hırsızlığı vb. vasıtasıyla çeşitli mali dolandırıcılıklar gerçekleştirilebilir.*
	Oltalama	*Oltalama (Kimlik avı) yolu ile, suçlular diğer kullanıcıların oturum açma veya kimlik bilgileri ile sanal varlıklarını çalabilir,* *Sesli ve SMS kimlik avı metotlarını kullanarak sesler ve telefon numaraları gibi kişisel verileri izinsiz toplanabilir*
	Para Aklama	*Suçlular, suç gelirleriyle NFT gibi dijital varlıkları veya sanal para birimlerini satın alabilir ve bunları temiz varlıklar karşılığında satabilir ve bu şekilde paranın menşe kaynağı izleme kapasitesini kısıtlarlar.*
	Vergi Suçları	*Mali Takip ve vergilerden kaçınmak için, suçlular dijital varlıklar üzerinden belirsiz mülkiyet yapıları oluşturabilir*
	Sahtekarlık	*Suçlular dijital varlıkların fiyatları kandırma vasıtasıyla şişirebilir veya sahte sanal pazarlar oluşturabilir ve var olmayan ürünleri satarak diğer kullanıcıları dolandırabilirler.*

		Ayrıca sanal varlıkları çalmak için Sanal Evren'e kötü amaçlı yazılım da sokabilirler Bazı örnekler şunları içerir: kimliğe bürünme dolandırıcılığı, yatırım dolandırıcılığı, romantizm dolandırıcılığı, teknik destek dolandırıcılığı, sahte Metaverse dolandırıcılığı, NFT dolandırıcılığı, hediye dolandırıcılığı, ödeme dolandırıcılığı, iş dolandırıcılığı, akıllı sözleşme dolandırıcılıkları vb.
Mala Karşı İşlenen Suçlar	**Avatar'dan Hırsızlık**	*Önemli miktarda gerçek dünyadaki mali kayıplar neden olacak şekilde suçlular sanal varlıkları veya parasal kazanç elde etek için anonim olarak sanal mülkleri çalabilirler. Ayrıca çoğaltmak, yeniden satmak veya değerini düşürmek için kültürel varlıkları da çalabilirler*
	Dijital Mallar ve Varlıkların Çalınması	
	Sanal Hırsızlık	*Sanal Evrendeki kişisel alana izinsiz girişler siber takip, tacize ve hatta kimlik hırsızlığına yol açabilir. Parasal kazanç için, suçlular, oyun içi işlemlerle bağlantılı sanal varlıkları çalabilir veya iş operasyonlarını kesintiye uğratabilir.*
	Özel Sanal Alana İzinsiz Girme	
	Mala Zara Verme	*Suçlular sanal etkinlikleri bozabilir, belirli kullanıcıları gasp etmek için hedefleyebilir veya sanal mülklere zarar vererek ve sanal vandalizm ile kaosa neden olabilir. Kişisel, politik veya ideolojik motivasyonlar ile suçlular sanat eserleri gibi kültürel varlıklara da zarar vermektedir.*
Telif Hakları Suçları	**Telif Hakkı İhlali**	*Suçlular sanal pazar yerlerinde desen ve marka ihlali yapmak suretiyle telif hakkıyla korunan NFT çalışmalarını kopyalayabilir veya satabilir. Görsellerin telif hakkı, videolar, yazılı prodüksiyonlar ve sahte ürünler bir kara para aklama tekniği olabilir ve aynı zamanda sanal ekonominin bozulmasına da yol açacaktır.*
	Sahtecilk	

Cinsel Suçlar ve Saldırı	**Saldırı**	*Suçlular, kişilerin kullandıkları avatarlarını rızası olmadan cinsel içerikli illegal saldırı yapmak ve taciz etmek için diğer kullanıcılarla sanal etkileşimlerde bulunabilirler.* *Bu, taciz olaylarından, açık cinsel içeriğin oluşturulması ve dağıtımına kadar değişebilir.*
	Cinsel Suistimal	
	Taciz	
	Cinsel Sömürü	
	Uygunsuz Teşhir	
Çocuklara Karşı İşlenen Suçlar	**Cinsel Sömürü**	*Suçlular çocukları manipüle edebilir, tehdit edebilir ve kendileri hakkında açıkça cinsel içerik yaratmaya zorlayabilirler. Suçlunun avatarı da cinsel taciz ve istismar yapabilir ve çocuklara karşı avcı davranışlar da bulunabilir ve haptik cihazların* kullanımıyla fiziksel vücutlarına etki yaratma potansiyeli vardır.* **Haptik teknolojisi, kullanıcıya kuvvetler, titreşimler veya hareketler uygulayarak bir dokunma deneyimi yaratabilen teknolojidir. Bu teknolojiler, bir bilgisayar simülasyonunda sanal nesneler oluşturmak, sanal nesneleri kontrol etmek ve makine ve cihazların uzaktan kontrolünü geliştirmek için kullanılabilir.* (Kaynak wikipedia)*
	Cinsel Taciz	
	İstismar için Çocuk Bakımı	*Çocuklar kötü niyetli aktörler tarafından para kazanmak için oyunlar ve sanal deneyimler yaratmak için kullanılabilir. Bu kötü niyetli aktörler, çocuklara daha fazla para kazanmak için daha fazla çalışmaları için baskı yapabilirler, ki bu sonuçta onlara verilmeyebilir. Bu, istismar ve çocuk işçiliğine yol açabilir.*
	Çocuk İşçiliği	
Siber Suçlar	**Bilişim ve bilgi sistemlerine hukuka aykırı bir şekilde girme ve müdahale etme**	*Suçlular veri çalmak, kullanıcıları tehdit etmek, sanal varlıkları talep etmek, bilgiyi manipüle etmek veya üçüncü taraf varlıklarını satmak için Metaverse platformlarını kullanabilirler.* **İfşa: bir birey veya kuruluş hakkında kişisel olarak tanımlanabilir bilgilerin, genellikle İnternet aracılığıyla ve onların rızası olmadan kamuya açık olarak sağlanması eylemidir. (Kaynak: Wikipedia)*
	Veri Hırsızlığı	
	Fidye Yazılım	
	İfşa*	

Korku/Dehşet ya da duygusal sıkıntıya yol açan eylemler ve suçlar	**Taciz**	*Suçlular kullanıcıları hassas bilgileri ifşa ve çevrimiçi şiddet uygulamakla tehdit edebilirler. Haptik geri bildirim gibi gelişmekte olan teknolojiler, kullanıcıların fiziksel ve psikolojik güvenliği konusunda endişe yaratarak yeni kötüye kullanım şekillerine izin verebilir.*
	Takip	*Suçlular, diğer kullanıcıların sanal varlığını, faaliyetlerini, ilgi alanlarını ve kişisel bilgilerini yakından takip edebilir ve gizliliği ve özel alanını ihlal edebilirler.*
	Samimi görüntülerin rıza dışı paylaşımı	*Suçlular, izni olmadan bir kişinin vücudunun, samimi veya sahte resimlerini paylaşabilir ve yayabilirler.*
	İftira/Karalama	*Avatar'a karşı yapılan bir iftira iddiası, kişinin gerçek dünyada kimliğini ve itibarını etkileyebilir.*
	Gasp ve Şantaj	*Suçlular kullanıcılardan belirli kişisel bilgileri toplayabilir ve şantaj ve istismar amaçlı kullanabilirler. Suçlular ayrıca yetkili kişiler ya da hükümetler/hükümet görevlileri gibi davranabilirler.*
Terörizm	**Siber-Fiziki Saldırı**	*Dijital ikiz teknolojisi kullanarak, tehdit aktörleri siber fiziksel saldırılar için kritik altyapı sistemlerine yasadışı erişim ve kontrol elde edebilirler.*
	Terörizmin Finansmanı	*Teröristler, terör amaçlı mali destek almak için Sanal Evren'i kötüye kullanabilirler, bu da terör saldırılarına, silahların yayılmasına veya organize suç gruplarının ve terör ağlarının güçlendirilmesine yol açabilir.*
	Radikalleşme ve Beyin Yıkama	*Teröristler Sanal Evrren'i çevrimiçi eleman temini, radikalleşme, eğitim ve bireylerin doktrinasyonu için kullanabilirler. Ayrıca anonim olarak fon toplayabilirler ve kısa bir süre içinde küresel bir seyirciye ulaşan sahte bilgi ve propagandayı kolayca yayabilirler.*
	Terörist grupların faaliyetleriyle ilgili koordinasyon, prova ve diğer eylemler	*Siber terörle uğraşan kullanıcılar dijital ikiz kullanılarak daha iyi koordinasyon ve uygulama ile gerçek dünya saldırılarına yol açabilirler.*
Kamu Güvenliğine Karşı	**Yanlış Bilgilendirme ve Dezenformasyon**	*Yanlış bilgi ve dezinformasyon, Metaverse'de kolayca yayılabilir, potansiyel olarak kamuoyunu manipüle edebilir ve kullanıcıların finansal*
	Propaganda Yapmak	

İşlenen Suçlar		*kayıplardan sosyal sorunlara ve ideolojik bölünmelere kadar uzanan sonuçlarla yanıltıcı ve bilgisi olmayan kararlar almasına neden olabilir.*
	Uyuşturucu Kaçakçılığı	*Kötü niyetli aktörler Metaverse aracılığıyla uyuşturucu ve narkotik içerikli metaları satabilir ve daha geniş bir müşterilere anonim olarak ulaşabilirler. Uyuşturucu kaçakçılığı bağımlılık sorunlarına yol açabilir ve toplumlara ve kamu güvenliğine zarar verebilir.*

BÖLÜM III

METAVERSE'DE ADLİ BİLİŞİM VE İNCELEME

Kullanımının artmasıyla birlikte, Metaverse, araştırmacılar için çok önemli bir veri ve delil kaynağı olarak ortaya çıkacaktır.

Bu nedenle, kolluk kuvvetleri kendilerini şunlara hazırlamalıdır:

(1) VR başlıklarından ve temasa dayalı cihazlardan veri erişimi;
(2) Metaverse altyapısından delil kurtarma;
(3) Üçüncü taraf Metaverse hizmet sağlayıcılardan veri elde etme;
(4) İlk müdahale ekiplerini, adli uzmanları ve tüm suç adalet sistemini eğitmek.

Teknoloji ve Cihazlar

Metaverse'in fiziksel dünyaya entegrasyonu veya tezahürü, başlıca Artırılmış Gerçeklik (AR) ve Nesnelerin İnterneti (IoT) gibi teknolojiler aracılığıyla çeşitli yollarla gerçekleştirilebilir. Bilgi veya sanal nesneler, fiziksel çevremize eklenmiş olabilir. Örneğin, AR gözlükleri veya lensleri, yönlendirme talimatları, fiziksel nesneler hakkında bilgi veya gerçek dünya konumlarıyla sanal etkileşimleri mümkün kılabilir. İnsanlar, AR aracılığıyla fiziksel olarak Metaverse ile etkileşimde bulunabilirler, örneğin sanal nesneleri manipüle etmek için el jestleri kullanabilir veya sanal olayları dokunsal bir şekilde deneyimlemek için uzamsal ses ve dokunmatik geribildirim kullanabilirler.

Fiziksel alanlara gömülü IoT cihazları, Metaverse'deki sanal alanlarla senkronize edilebilir, bu sayede her iki dünya arasında gerçek zamanlı veri akışını sağlar ve potansiyel olarak fiziksel ortamların sanal etkileşimler aracılığıyla kontrol edilmesine imkan tanır. Giyilebilir cihazlar, kullanıcının fiziksel durumuna bağlı olarak avatarın görünümünü, davranışını veya yeteneklerini etkileyerek gerçek zamanlı biyometrik verileri Metaverse'e aktarabilir. Giyilebilir cihazlar ayrıca Metaverse'deki avatarın deneyimlediği fiziksel hisleri taklit etmek için dokunsal geri bildirim sağlayabilir ve sanal ve fiziksel deneyimler arasında somut bir bağlantı sağlayabilir. Metaverse'de oluşturulan tasarımlar veya nesneler, 3D baskı teknolojileri aracılığıyla da fiziksel dünyaya taşınabilir.

Geleneksel adli yakalama yöntemlerini kullanarak Metaverse'deki suçları araştırmak, dağıtılmış defterlerin benimsenmesi, blockchain teknolojisi, kripto para birimi ve merkezi olmayan yönetim gibi Metaverse'de benimsenen yeni teknolojiler nedeniyle kolluk kuvvetleri için çeşitli zorluklar doğurmaktadır.

Son Nokta Adli Bilişim

Çoğu suç soruşturmasında ve dijital adli bilişim incelemelerinde, suça karışmış bir cihazın, suçu kolaylaştırmak için mi yoksa suç mağduru olarak mı kullanıldığının, suç bildirildikten sonra kimliklendirilmesi ve doğrulanması gerekir. Modern suç soruşturmalarının çoğunda, günlük yaşamda çoğunlukla, akıllı telefonlar, diğer akıllı cihazlar ile internet gibi, teknolojinin kullanılması nedeniyle, dijital bir unsura rastlanmaktadır. Dijital adli bilişim, çeşitli alanlarda soruşturmalara yardımcı olmak için kullanılabilen güçlü bir araçtır. Doğru ve güvenilir kanıtlar sunarak, dijital adli bilişim, soruşturmacılara fail tespiti ve kovuşturma, çalınan veya kaybolan verilerin kurtarılması ve gelecekteki suçların önlenmesinde yardımcı olabilir. **Dijital adli bilişim, sistematik veri toplama, silinmiş veya gizlenmiş verilerin kurtarılması, kapsamlı veri analizi, olayların yeniden yapılandırılması, saldırganın tespiti ve gelecekteki olayları önlemek ve hafifletmek için ardışık aşamalar içeren bir prosedür çerçevesini içermektedir.**

Çoğu verinin platformlarda depolanması nedeniyle, Metaverse'te son nokta adli bilişim sınırlıdır. Son nokta adli bilişim, tek bir cihaz veya sistem içinde meydana gelen olayları araştırmak için kullanışlı olabilir, ancak Metaverse'te meydana gelen olayları inceleme konusunda birkaç kısıtlamaya sahiptir. Araştırmacılar ve dijital adli inceleyiciler için Metasuç soruşturması yapılırken kullanışlı olabilecek son nokta cihazları şunlar olabilir:

- VR Başlıkları ve diğer giyilebilir teknolojiler
- Bilgisayar/Dizüstü bilgisayar
- Mobil Telefon
- Yönlendiriciler
- Akıllı Cihazlar

Son Nokta Adli Bilişim Zorlukları

- **Standardizasyon eksikliği:** Metaverse, standartlaştırılmış protokol ve yapılardan yoksun, karmaşık ve hızla gelişen bir dijital ortamdır. Farklı Metaverse platformları farklı günlük kaydı ve veri toplama mekanizmalarına sahip olabileceğinden, bu durum son nokta adli bilişiminin tutarlı ve güvenilir bir şekilde yürütülmesini zorlaştırır.
- **Dağıtılmış yapı:** Metaverse'deki olaylar genellikle çok çeşitli ağlara ve platformlara dağıtılmış birden fazla cihaz ve sistemi içerir. Son nokta adli bilişimi, tek bir son nokta cihazına odaklandığından ve olayın tam bir resmini sağlayamayabileceğinden, bu tür olayları araştırmak için yeterli olmayabilir. Veriler geçici olarak cihazda saklanabilir ve daha sonra uzun süreli koruma için merkezi bir bulut sunucusuna aktarılabilir.
- **Verilerin çıkarılmasındaki zorluklar:** Metaverse'deki soruşturmalar büyük miktarda kişisel verinin toplanmasını ve analiz edilmesini içerebilir; bu da gizlilik

ve veri korumayla ilgili endişeleri artırabilir. Son nokta adli bilişimi, soruşturmaya katılan bireylerin mahremiyet ve veri koruma haklarına saygı gösterirken olayın tam bir resmini sağlayamayabilir. Bu bağlamda, araştırma amacıyla VR başlığından ek bilgi almak amacıyla uygun ayrıcalıkların edinilmesi gerekli olabilir.

- **Fiziksel kanıt eksikliği:** Metaverse'de olaylar genellikle sanal varlıkları ve dijital etkileşimleri içerir; bunlar, son nokta adli bilişimi kullanılarak toplanabilecek ve analiz edilebilecek fiziksel kanıt bırakmayabilir. Bu durum, olaya yol açan olayların sırasının belirlenmesini ve olaya karışan tarafların tespit edilmesini zorlaştırmaktadır.
- **Teknik zorluklar:** Metaverse teknik açıdan karmaşık bir ortamdır ve araştırmalar, çoğu araştırmacının kolayca erişemeyeceği özel bilgi ve araçlar gerektirebilir.
- **Adli Tıpa Karşı Metaverse:** Geçici veri depolama ve dinamik ortamlar için tasarlanmış platformların kullanılması, kanıtların hızla kaybolmasına veya değiştirilmiş gibi görünmesine neden olabilir.
- **Çoklu Yargı Alanı Hususları:** Merkezi olmayan yönetim ve bulut sunucularının farklı yetki alanlarında bulunması nedeniyle, sunucunun geçerli olduğu yasalar, Metaverse ile ilgili soruşturmaları ve elde edilen adli kanıtların toplanmasını ve kullanılmasını etkileyebilir. Farklı hukuk sistemleri, mevzuat ve kişi anlayışlarının ilgili tüm kişilerin Metaverse'de işlenen suçların başarılı bir şekilde soruşturulması ve kovuşturulması üzerinde etkisi vardır.

Özetle, son nokta adli bilişim, standartlaştırma eksikliği, dağıtık yapısı, gizlilik ve veri koruma endişeleri, fiziksel delil eksikliği ve içerdiği teknik zorluklar nedeniyle Metasuç'ları soruşturmak konusunda birçok kısıtlamaya sahiptir. Bu nedenle araştırmacılar, Metaverse'deki olayları etkili bir şekilde soruşturmak için ağ adli bilişim, sosyal mühendislik ve özel araçlar ve teknikleri içeren bir kombinasyon kullanmak zorunda kalabilirler.

Kaynak: Lexica.com

Sunucu Soruşturmaları ve Adli Bilişim

Sunucu adli bilişim, bir sunucunun ele geçirilip ele geçirilmediğini belirlemek, bir Metasuç'un nedenini belirlemek veya belirli bir kullanıcı veya etkileşim etrafında belirli kanıtları kurtarmak için yapılan bir süreçtir. Sunucu adli bilişimin temel amacı, olayın kök nedenini belirlemek ve gelecekteki olayları önlemek veya belirli bir kullanıcı etrafında özel veri elde etmeye yardımcı olmak için dijital delilleri toplamak ve analiz etmektir.

Sunucu adli bilişim sırasında, araştırmacılar genellikle dijital delilleri tanımlama ve koruma, ne olduğunu belirlemek için delilleri analiz etme ve bulgularını açık ve özlü bir şekilde sunma sürecini takip ederler. Sunucu adli bilişim, yetkisiz erişim, veri ihlalleri, kötü amaçlı yazılım enfeksiyonları ve sistem arızaları gibi geniş bir olay yelpazesini araştırmak için kullanılabilir.

Genel olarak, sunucu adli bilişim, güvenlik olaylarını araştırmak ve organizasyonların dijital varlıklarını korumak için kritik bir araçtır. Bu sunucu delillerinin çoğu, eğer varsa, genellikle yargı veya kolluk kuvveti eyleminin bir parçası olarak üçüncü taraf bir şirketten temin edilmelidir. Bu üçüncü taraf sunucuları, genellikle Metaverse ev sahibi tarafından büyük veri merkezlerinde güvenli bir şekilde saklanmaktadır ve adli muayene yapma izni genellikle verilmez.

Dikkate alınması gereken bazı konular şunlar olabilir:

- Barındırılan sunuculardan silinen verileri kurtarmak için SSD teknolojisi,
- Elektronik varlıkların ve kağıt varlıkların (mobil cihazlar, Nano Ledger gibi elektronik defterler, e-Cüzdanlar, tohum ifadeler, mobil cihaz sorgulama, yedekler, şifreleme mekanizmaları gibi) el konulması.
- Şüphelilerle görüşmeler ve tanık ifadelerini almak için kolluk kuvvetleri tarafından benimsenen yaklaşım. Metaverse hala gelişmekte olduğundan, dijital araştırmacıların sağlam teknikleri benimsemek için dikkatli olmaları ve özel dijital ve adli suç birimlerini desteklemeleri önemlidir.

Metaverse Platformları

Dijital platform adli bilişim, sosyal medya siteleri, mesajlaşma uygulamaları ve bulut tabanlı hizmetler gibi dijital platformları araştırmayı içeren dijital adli bilişimin bir dalıdır. Dijital platform adli bilişimin amacı, Metasuç'ın nedenini belirlemek, olaya dahil olan tarafları tanımlamak ve yasal süreçlerde kullanılabilecek delilleri sağlamaktır.

Dijital platform adli bilişimin bir zorluğu, dijital platformların sürekli olarak gelişiyor olmasıdır; düzenli olarak yeni özellikler ve işlevsellikler eklenir. Bu, araştırmacıların bu platformlardaki olayları etkili bir şekilde soruşturabilmek için en son araç ve teknikler konusunda güncel olmalarını gerektirir.

Genel olarak, dijital platform adli bilişim, dijital platformlardaki Metasuç olaylarını soruşturmak için kritik bir araçtır ve organizasyonlara ve kolluk kuvvetlerine suçluları tanımlama, delil toplama ve siber suçluları kovuşturma konusunda yardımcı olabilir.

Bir örnek olarak, bazı sosyal medya platformları, kullanıcılara profil, etkileşimler, arkadaş listesi, sohbet mesajları, fotoğraflar, videolar ve diğer veri türlerini indirme olanağı tanır. Eğer bu amaçla bir standart işlem prosedürü varsa, kolluk kuvvetleri bu verileri kullanabilir. Bu yaklaşım, kullanıcılara rahatsızlık vermemeyi ve kolluk kuvvetlerinin hizmet sağlayıcılardan ve platformlardan talep ettiği bilgi miktarını sınırlamayı amaçlar.

Blockchain Adli Bilişimi

Blockchain adli bilişim, blockchain tabanlı işlemler ve faaliyetlerin araştırılmasına odaklanan dijital adli bilişimin bir dalıdır. Blockchain, ağ üzerinde gerçekleşen tüm işlemlerin ve faaliyetlerin değiştirilemez bir kaydını sağlayan merkezi olmayan bir defter teknolojisidir. Bu nedenle, blockchain adli bilişim, blockchain ağlarından dijital delillerin toplanması ve analizini içerir ve sahtekarlık veya suç faaliyetlerini araştırmayı amaçlar.

Blockchain adli bilişimin ana uygulama alanlarından bazıları, kripto para birimlerinin dahil olduğu Metasuçlar soruşturmasıdır; bu tür suçlar arasında para aklama, dolandırıcılık ve şantaj yer alabilir. Araştırmacılar, blockchain ağlarından dijital delilleri toplamak ve analiz etmek için çeşitli teknikleri kullanabilirler; bunlar arasında işlem kayıtlarını analiz etmek, cüzdan adreslerini incelemek ve farklı adresler arasındaki fon akışını izlemek bulunabilir.

Blockchain adli bilişimin ana zorluklarından biri, blockchain işlemlerinin dağıtık ve takma adlı doğasıdır. Geleneksel finansal işlemlerin aksine, blockchain işlemleri kullanıcılardan kişisel bilgi sağlamayı gerektirmez, bu da bir işleme dahil olan tarafları tanımlamayı zorlaştırabilir. Ayrıca, blockchain ağları şeffaf olacak şekilde tasarlanmıştır, bu da herkesin blockchain defterinin içeriğini görebileceği anlamına gelir, ancak bu aynı zamanda hassas bilgilerin gizliliğini korumayı zorlaştırır.

Genel olarak, blockchain adli bilişim, blockchain teknolojisinin giderek daha yaygın bir şekilde benimsenmesiyle birlikte giderek daha önemli hale gelen hızla büyüyen bir alandır. Blockchain ile ilgili suçları soruşturmak ve kovuşturmak için gerekli araçları ve teknikleri sağlayarak, blockchain adli bilişim, blockchain ağlarının bütürlüğünü korumaya ve teknolojinin kötüye kullanılmasını önlemeye yardımcı olabilir.

Kripto Para Analitiği

Kripto para analitiği, kripto para işlemlerini inceleyip analiz etme alanını içeren bir alandır ve bu analizlerle para aklama, dolandırıcılık ve şantaj gibi yasa dışı faaliyetlerde bulunan bireyleri tespit etmeyi amaçlar. Kripto paralar, dijital veya sanal paralardır ve para birimi birimlerinin üretimini düzenlemek ve fon transferini doğrulamak için şifreleme tekniklerini kullanır.

Kripto para işlemlerinin incelenmesi, temel blockchain teknolojisi ve çeşitli kripto para protokollerine derin bir anlayış gerektirir. Araştırmacılar, kripto para işlemleri kayıtlarını, cüzdan adreslerini ve diğer dijital artefaktları analiz etmek için özel araçlar ve teknikler kullanırlar, böylece yasa dışı faaliyetlere işaret eden desenleri ve anormallikleri tespit edebilirler.

Kripto para analitiğinin yaygın uygulamalarından bazıları, fidye yazılım saldırıları, karanlık web pazarları ve kripto paraların kullanıldığı diğer siber suç biçimlerinin soruşturulmasıdır. Kripto para analitiği, aynı zamanda kripto paraların transfer edilmesinde kullanılan dolandırıcılık veya zimmete para geçirme vakalarını incelemek için de kullanılabilir.

Kripto para analitiğinin temel zorluklarından biri, kripto para işlemlerinin anonim doğasıdır. Bitcoin ve Ethereum gibi kripto paralar, kullanıcıların kimlik bilgisi sağlamadan cüzdan adresleri oluşturabilmesini içerir. Bu durum, bir işleme dahil olan tarafları belirlemeyi zorlaştırabilir, ancak araştırmacılar cüzdan adreslerini belirli bireylerle bağlantılı hale getirmek için çeşitli teknikleri kullanabilirler.

Kripto paranın yaygınlaşması ve daha erişilebilir hale gelmesiyle, mevcut kripto para soruşturma metodolojisinin, kripto para teknolojisinin çektiği yenilikçi ortama uyum sağlaması gerekebilir.

Değiştirilemeyen Token (NFT) Adli Bilişimi

NFT adli bilişimi, değiştirilemeyen token'ların (NFT'ler) incelemesi ve analizi ile ilgilenen dijital forensik bir alanı ifade eder. NFT'ler, bir blockchain üzerinde depolanan benzersiz dijital varlıklardır ve sanat dünyası ve diğer yaratıcı endüstrilerde giderek daha popüler hale gelmektedir. 2023 Aralık ayında, bir üye ülkenin NFT ile ilgili suçları ele alan Mor Bildirim yayınlandı.

Bazı yazılım mimarları, NFT'leri Metaverse'lerin temel bir bileşeni olarak düşünerek varlıkların platformlar arasında taşınabilirliğini sağlamayı mümkün kılabilir. Taşınabilir NFT varlıklarının bazı örnekleri şunları içerebilir:

- **Sanal gayrimenkul:** Sanal dünyalarda veya Metaverse'lerde, NFT'ler sanal arazi sahipliğini temsil edebilir. Bu sanal arsalar fiziksel emlak gibi alınıp satılabilir ve geliştirilebilir.
- **Dijital sanat ve koleksiyonlar**: NFT'ler, dijital sanat dünyasında sanatçıların eserlerini yeni yollarla paraya çevirmelerine olanak tanıyarak büyük bir etki yaratmıştır. Metaverse'de bu sanat eserleri, sanal galerilerde veya evlerde sergilenerek gösterilebilir.
- **Sanal ürünler:** NFT'ler, giyim, mobilya, araçlar vb. gibi sanal ürünleri temsil edebilir. Kullanıcılar bu öğeleri Metaverse içinde kullanmak için satın alabilirler.
- **Kimlik ve itibar:** NFT'ler, benzersiz dijital kimlik oluşturmak için potansiyel olarak kullanılabilir. Bu, Metaverse içinde gösterilebilecek başarılar, beceriler veya deneyimlerin kanıtlarını içerebilir.
- **Deneyimler ve erişim:** NFT'ler, Metaverse içindeki sanal konserlere, konferanslara, buluşmalara veya diğer deneyimlere bilet olarak kullanılabilir. Ayrıca, Metaverse içindeki özel alanlara veya kulüplere erişim sağlayabilirler.
- **Oyun varlıkları:** Metaverse içindeki video oyunlarında, NFT'ler oyun varlıklarını temsil edebilir. Bu, silahlar, zırh, karakterler ve evcil hayvanlar gibi her şeyi içerebilir.
- **Fikri Mülkiyet:** NFT'ler ayrıca Metaverse içindeki fikri mülkiyet haklarını yönetmek ve transfer etmek için kullanılabilir, örneğin bir müziğin, bir filmin veya bir markanın hakları.

NFT adli bilişimi, NFT işlemleri ve etkinlikleriyle ilgili dijital delillerin toplanması ve analizi ile ilgilenir. Bu, blockchain işlem kayıtlarını analiz etmek, NFT'lerin meta verilerini incelemek ve NFT'lerin farklı adresler arasındaki akışını izlemek gibi konuları içerebilir.

NFT adli bilişimi uygulamalarından biri, sahte NFT'lerin oluşturulması ve satılması gibi NFT dolandırıcılığı vakalarını soruşturmak içindir. Araştırmacılar ayrıca, NFT'leri içeren telif hakkı ihlalleri ve fikri mülkiyet hırsızlığı vakalarını incelemek için de NFT adli bilişimi kullanabilirler.

NFT adli bilişimi'nin zorluklarından biri, blockchain ağlarının karmaşık ve merkezi olmayan yapısıdır, bu da bir NFT işleminde yer alan tarafları belirlemeyi zorlaştırabilir. Ayrıca, bir NFT'nin orijinal yaratıcısını belirlemek veya bir NFT'nin içinde genellikle resimler, videolar ve diğer multimedya dosyaları gibi geniş bir dijital içerik yelpazesi bulunduğu için bir NFT'nin doğruluğunu belirlemek zordur.

NFT adli bilişimi, NFT'lerin kullanımının arttıkça giderek daha önemli hale gelen hızla büyüyen bir alandır. NFT adli bilişimi, polise, NFT'leri içeren suçları soruşturmak ve kovuşturmak için gerekli araçlar ve bilgiyi sağlayarak NFT pazarlarının bütünlüğünü korumaya yardımcı olabilir.

Kaynak: Lexica.com

Metaverse Hizmet ve Platform Sağlayıcıları

Hukuk uygulayıcılar için, hizmet ve platform sağlayıcılardan veri talep etmek, soruşturmalara yardımcı olmak için yaygın bir uygulamadır. Hukuk uygulayıcı ajanslar, genellikle bir sağlayıcıya yazılı talep (mahkeme kararı, arama kararı, üretim emri veya mahkeme kararı gibi) sunarak veri talep etme eğilimindedirler. Bu tür taleplerde bulunmak için belirli bir prosedür ve gereksinimler, yargı alanına ve talep edilen bilginin türüne bağlı olarak değişebilir.

Hukuk uygulayıcı ajanslarının, veri talebinde bulunurken uygun hukuki prosedürleri takip etmeleri, herhangi bir yasal zorluk veya diğer sorunlarla karşılaşmamak için önemlidir. Ayrıca, bilgiye erişim ihtiyacı ile bireylerin gizlilik ve hukuki süreç hakları arasında denge kurmak önemlidir.

Metaverse sağlayıcılarından veri talebinde bulunurken hukuk uygulayıcılarının karşılaştığı başlıca zorluklardan biri, çoğu zaman barındırma platformu tarafından depolanan veriler hakkında ne tür bilgi talep edilebileceğini anlamaktır. Bir platformun belirlenmesinden sonra, talep edilen verilerin elde edilebilmesi için hukuk uygulayıcıların platform ile etkileşimde bulunmaları önemlidir. Ayrıca, her bir talep belirli bir süreç ve sınırlamalara tabi olacaktır. Örneğin, bazı sosyal medya platform sağlayıcıları, belirli verileri sınırlı bir süre için saklayabilir. Bu nedenle, bir hesap belirlendikten sonra, verilerin ve etkinlik ilgilerinin silinmesini sınırlamak için mümkün olan en kısa sürede bir koruma talebinde bulunulması önemlidir.

Metaverse, hukuk uygulayıcıları için iki temel unsuru belirleme konusunda çeşitli zorluklarla karşılaşacaktır: **yargı ve atıfta bulunma**. Bu zorluklar, geleneksel siber suçlarla benzerdir, ancak Metaverse, başka bir karmaşıklık katmanı ekleyecektir.

Metaverse ile ilgili bir dizi hukuki zorluk, gelecek yıllarda yargılanacak olan davalarla ilgili olacaktır. Hukuk uygulayıcı ve hukuk topluluklarının teknoloji hakkında bilinçli olmalarını ve bu alanda uzmanlığa sahip olmalarını sağlamak önemlidir.

Büyük Dil Modelleri ve Diğer Üretken Yapay Zeka Teknolojileri

Metaverse'i üretken yapay zeka teknolojileri ve büyük dil modelleriyle inşa etmek, geniş sanal ortamlar, dinamik anlatılar ve çeşitli oyuncu olmayan karakterlerin (NPC'ler) cazip bir vizyonunu sunar. Ancak, bu Yapay Zeka teknolojilerinin "siyah kutu" olarak sıklıkla kabul edilen potansiyel suç riskleri ve öngörülemeyen doğası konusunda farkında olmak kritiktir.

- **Dünya Oluşturma:** Yapay zeka, bütün şehirlerden bireysel mobilya parçalarına kadar çeşitli sanal ortamlar oluşturabilir. Ancak, Yapay Zeka'nın yasa dışı faaliyetlere elverişli ortamlar yaratma riski bulunmaktadır. Doğru bir şekilde yönetilmezse, bu ortamlar sanal hırsızlıktan daha ciddi suçlara kadar, suçlara yanlışlıkla zemin hazırlayabilir veya teşvik edebilir.
- **Oyuncu Olmayan Karakterler (NPC'ler):** GPT-3 gibi Yapay Zeka, NPC'ler için benzersiz kişilikler ve davranışlar üretebilir, ancak bu karakterlerin suç amaçları için manipüle edilme riski vardır. NPC'ler, zararlı eylemleri gerçekleştirmek, yasa dışı materyalleri dağıtmak veya diğer kullanıcıları aldatmak için sömürülebilir.
- **Dinamik Hikayeler:** Yapay zeka, kullanıcı etkileşimlerine dayalı kişiselleştirilmiş hikayeler oluşturabilir. Ancak, bu potansiyel olarak bireylere zararlı içerikle hedeflenmek veya kullanıcıları kişisel bilgileri ifşa etmeye veya yasa dışı faaliyetlere katılmaya yönlendirmek için kullanılabilir.
- **İçerik Moderasyonu:** Yapay Zeka, içeriği izlemeye ve düzenlemeye yardımcı olabilir, ancak kusursuz değildir. Kötü niyetli kullanıcılar, bu sistemleri atlamak için yollar bulabilir ve zararlı içeriği yaymak veya suç işlemek için kullanabilir.

Birçok Yapay Zeka modelinin "siyah kutu" doğası, bu riskleri artırır. Bu modellerin giriş ve çıkışlarını gözlemleyebiliriz, ancak iç çalışma mekanizmaları anlaşılamayan ve karmaşık yapılara sahiptir. Bu, beklenmeyen ve potansiyel olarak zararlı sonuçlara neden olabilir. Örneğin, bir Yapay Zeka, suç faaliyetlerini kolaylaştıran bir ortam veya NPC davranışı üretebilir, ancak insan tasarımcılar bunun farkında olmayabilir.

Ayrıca, Yapay Zeka modelleri, eğitim verilerinde bulunan önyargıları yansıtabilir ve yayabilir. Dikkatlice düzenlenmezse, bu veri, zararlı veya yasa dışı içerik içerebileceğinden, Yapay Zeka'yi Metaverse içinde benzer içerikler üretmeye yönlendirebilir.

Büyük Dil Modelleri (LLM) ve Yapay Zeka teknolojilerinin "siyah kutu" doğası, suç soruşturmaları için bir dizi zorluk ortaya çıkarabilir:

İzlenebilirlik: Yapay Zeka modellerinin karar verme süreçleri kolayca yorumlanamadığından, belirli bir çıkışın veya eylemin kökenlerini izlemek zor olabilir. Bu, Metaverse'teki bir suçun bir Yapay Zeka tarafından mı yoksa bir insanın Yapay Zeka'yi sömürdüğü bir eylem tarafından mı gerçekleştirildiğini belirlemeyi zorlaştırabilir.

Öngörülebilirlik: Yapay Zeka davranışlarının öngörülemezliği, yasa dışı faaliyetlerin önceden tahmin edilememesine ve önlenememesine neden olabilir. Örneğin, bir Yapay Zeka'nın yanlışlıkla suç faaliyetlerini kolaylaştıran bir ortam oluşturması, ancak bu durum sadece olaydan sonra anlaşılırsa bu durumun bir örneğidir.

Sorumluluk: Eğer bir suç, bir Yapay Zeka'nın yardımıyla işlenirse (örneğin, bir NPC'nin zararlı eylemleri gerçekleştirmesi durumunda), hukuki sorumluluğun kimde olduğunu belirlemek zor olabilir. Temel soru, Metaverse bağlamında (yani, Yapay Zeka'nin tasarımcıları, Metaverse operatörleri, Yapay Zeka'yi manipüle eden bireysel kullanıcı veya bunların bir kombinasyonu) kimin sorumlu veya hesaplı olduğudur.

Veri gizliliği: Soruşturmalar genellikle veri toplama ve analizine dayanır. Ancak, Yapay Zeka teknolojileri, gizlilik haklarına zarar verebilecek şekillerde veri üretebilir veya işleyebilir. Örneğin, bir Yapay Zeka'nin suçu önlemek için Metaverse içinde kullanıcı davranışını izlemek için kullanılması, gözetim ve veri kötüye kullanımı konusunda endişelere yol açabilir.

Önyargı ve ayrımcılık: Eğer Yapay Zeka teknolojileri, eğitim verilerinde bulunan önyargıları yansıtıyorsa, bu, suç soruşturmalarını etkileyebilir. Örneğin, belirli kullanıcılar veya faaliyetler, önyargılı Yapay Zeka davranışı nedeniyle haksız bir şekilde hedef alınabilir veya gözden kaçırılabilir.

Uluslararası ve Yargısal konular:

Metaverse'in küresel doğası nedeniyle, içinde işlenen suçlar birden çok ülkeden katılımcıları içerebilir. Bu durum, Yapay Zeka teknolojilerinin dahil olması durumunda, Yapay Zeka ve siber suçlarla ilgili uluslararası yasalara ve düzenlemelere olan farklılıklar nedeniyle suç soruşturmalarını karmaşıklaştırabilir.

Uygulamalara, platformlara ve Metaverse'e erişim sağlayan cihazlara entegre oldukça, soruşturmacı ve adli inceleme uzmanları, LLM ve Yapay Zeka'nin Metaverse ve ilişkili platformlar ve uygulamalardaki kullanımı konusunda güncel kalmaları gerekecektir. Bu teknolojilerin suç veya soruşturmadaki kullanımını yorumlayabilmek için LLM ve Yapay Zeka'nin nasıl çalıştığını anlamalarını sağlamak önemlidir.

İlk Müdahaleciler, Dijital Adli Uzmanlar ve Yargı Sistemi Eğitimi

İlk müdahalecilerin, dijital adli uzmanların ve yargı sisteminin Metaverse, sanal ortamlar ve ilişkili teknolojiyi anlamaları, sanal ortamların güvenliğini ve güvenliğini sağlamak, bunları kullanan bireylerin haklarını korumak önemlidir. Sanal ortamlara ilişkin dijital delilleri incelemek ve analiz etmek için, kolluk kuvvetlerinin dijital adli konularda eğitim alması gerekmektedir. Sanal ortamları desteklemek için, sanal ve artırılmış gerçeklik teknolojilerinde, ayrıca blockchain ve diğer dağıtılmış defter teknolojilerinde özel eğitimler gerekebilir.

Ayrıca, yargı sisteminin, sanal ortamlarla ilgili vakaları değerlendirmeyi ve yargılamayı öğrenmesi gereklidir. Sanal ortamlarda ortaya çıkan zorluklar ve sorunlar konusunda yargıçlar, avukatlar ve diğer hukuk profesyonelleri için yeni hukuki çerçeveler ve standartlar geliştirmek, ayrıca bu konularda eğitim almak gerekebilir.

BÖLÜM IV

METAVERSE YÖNETİMİ

Metaverse'in ortaya çıkışı, toplumlarımız üzerindeki potansiyel önemli etkisi göz önüne alındığında, çok çeşitli yönetişim ve politika sorunlarını ortaya çıkarabilir. Bu sorunları anlamak ve düzenleyici çerçevedeki gerekli değişiklikleri düşünmek, ortaya çıkan bu teknolojinin gelişmesi için çok önemli olacaktır. Her politika seçeneğinin çeşitli paydaşlar üzerinde farklı etkileri olabileceğinden, düzenleyici çerçevede gerekli değişikliklerin belirlenmesi için çok paydaşlı bir yaklaşım gerekmektedir. Bu önemli tartışmaya bir temel sağlayan, bu bölümde, özellikle kolluk kuvvetleriyle ilgili olanlar olmak üzere birkaç temel politika konusu özetlenmektedir. Metaverse'in nasıl yönetildiğine bağlı olarak çeşitli modellerinin bulunduğunu da belirtmek önemlidir. Bu bölümde, hem merkezi hem de merkezi olmayan modeller dikkate alınarak Metaverse'in mevcut ve gelecekteki yönleri tartışılmaktadır.

Temel Yönetişim Sorunları

Metaverse'de Kimlik Yapısı

- Metaverse'deki pek çok suç faaliyetinde avatarlar, suçluların yararlanabileceği bir anonimlik sağlayabilir. Gerçek dünyadaki bireyler için vekil olarak kullanılabilirler ve çalıntı malları satın almak için sanal para birimlerini kullanabilirler. Tehdit aktörleri, sahte kimlikler oluşturmak ve insanları yasa dışı faaliyetlere katılmaya teşvik etmek için avatarları da kullanabilir.
- Metaverse'de bir hesap ve avatarlar oluştururken kimlik doğrulama gereksinimleri ve süreçleri farklılık gösterebilir. Bazı Metaverse platformları yalnızca bir kripto cüzdanı gerektirebilirken diğerleri e-posta adresleri veya ulusal kimlik numaraları isteyebilir. Kimlik doğrulamaya yönelik standartların veya gerekliliklerin daha düşük seviyede olması nedeniyle kolluk kuvvetleri, avatarlarının arkasında suç faaliyetlerine karışan kişilerin izini sürmek konusunda zorluklarla karşılaşabilir.
- Dikkate alınması gereken diğer bir husus, platformların kullanıcı kimliğine ilişkin topladığı bilgiler (kullanıcıdan hizmete) ile kullanıcıların kimlikleri hakkında diğer kullanıcılarla paylaştığı bilgiler (kullanıcıdan kullanıcıya) arasında ayrım yapılmasıdır. Kullanıcıların Metaverse içindeki bağlamlara ve kullanım durumlarına bağlı olarak farklı tanımlama modlarını tercih etmeleri de mümkündür.

Avatar nedir?

Uluslararası toplum, avatar kavramının tanımlanmasına yönelik tartışmalara devam ediyor. ITU'nun Metaverse Odak Grubu bünyesinde geliştirilen tanımlardan biri: "sanal ortamlarda kullanıcının (görsel) temsili olarak kullanılabilecek bir dijital varlık" tır. Ayrıca INTERPOL'ün bakış açısına göre avatarın tüzel kişilikleri şu şekilde düşünülebilir:

• İnsanın uzantısı; veya

• İnsanın sembolik temsili; veya

• İnsanın mülkiyeti; veya

• Özerk tüzel kişilik.

Avatarları algılama ve kabul etme şeklimiz, bunların dahil olduğu zarar ve suç faaliyetleri konusunda farklı sonuçlara yol açabilir. Bir avatarı eyleminden sorumlu tutmak, avatara tüzel bir kişilik atfetmek, avatarları bir hukuk sistemi içerisinde tanımak ve onların dava açma veya dava edilme gibi yasal işlemlere tabi tutulmasına izin vermek anlamına gelir.

Kovuşturmanın hukuki sonuçları ve olası sonuçları, avatarların tanımlarına ve tüzel kişiliklerine bağlı olarak farklılık gösterebilmektedir. Yasal bir avatar ile bu avatarı kontrol eden kullanıcı arasında ayrım yapmaya yönelik standartlar ve kriterlerin geliştirilmesi de önemli olacaktır. Bu bağlamda, avatarlara ilişkin ortak bir anlayış ve tanım geliştirmek ve bu ortamın ulusötesi doğası dikkate alındığında üye ülkeler arasındaki yasal boşlukları azaltmak için çeşitli paydaşlar arasında sürekli bir diyalog şarttır.

Veri yönetimi

Metaverse'i kullanırken, üretilen, toplanan, depolanan ve işlenen çok büyük miktarda veri vardır. Bu veriler biyometrik verilerin yanı sıra VR gözlük kullanan kullanıcıların duygusal ve fizyolojik tepkilerine ilişkin verileri de içeriyor. Ancak biyometrik ve yüz tanıma teknolojilerinin hızla benimsenmesi ve yaygınlaşması ile bunlara yönelik evrensel olarak kabul edilen standartların ve düzenlemelerin geliştirilmesi arasında bir gecikme var.15 Bu gecikme, gizlilik kaygıları ve farklı sektör ve bölgelerdeki boşluklar da dahil olmak üzere çeşitli zorluklara yol açabilir. Aynı zamanda, Metaverse'e dahil olan çok sayıda varlık da karmaşık bir ilişkiler ağı oluşturarak veri yönetimi açısından sorumluluk ve yükümlülüklerde belirsizliğe yol açar. Örneğin veri denetleyicisi ve veri işleyicisinin sorumluluk ve sorumluluğunun tanımlanması, kullanıcı verilerinin korunması ve mevcut verilere ve gizlilikle ilgili yasa ve düzenlemelere uygunluğun sağlanması açısından önemli olacaktır.

Yasalar ve Düzenlemeler

- Metaverse'de farklı yargı yasaları ve düzenlemeleri geçerli olabilir. Farklılıkları anlamak için mevcut yargı yetkisine dayalı sözleşme kanununun, mülkiyet kanununun, ceza kanununun, vergi kanununun ve diğer ilgili kanunların Metaverse'de nasıl uygulanabileceğini değerlendirmeye ihtiyaç vardır. Aynı zamanda, İnsan Hakları Evrensel Bildirgesi'nin ve mevcut diğer uluslararası yasaların Metaverse'de uygulanmasının sağlanması temel olacaktır.

- Yargısal bağlamın daha iyi anlaşılmasıyla, bu üç boyutlu dünyanın ulusötesi doğası göz önüne alındığında, metaversede veya Metaverse aracılığıyla zarara neden olan eylemlerin suç sayılması konusunda üye ülkeler arasındaki yasal ve düzenleyici boşlukların ele alınması daha mümkün olacaktır.

Metaverse'deki Zararları Ele Almak Amacıyla Müdahale İçin Bir Eşik Oluşturmak

- Fiziksel dünyaya benzer şekilde, bu üç boyutlu dünya, metaversede işlenen zararlara, ciddiyetlerine bağlı olarak tepki vermek için bir eşik gerektirir.
- İster fiziksel, ister psikolojik, ister hibrit zararlar olsun, bunları etkili bir şekilde azaltmak ve ele almak için zararın düzeyini anlamak ve tanımak önemlidir.
- Genel olarak bireylerden öncelikle kendi kendilerini düzenlemeleri, davranış ve eylemlerinin sorumluluğunu almaları beklenir. Yoğunlaşan etkileşimlerle birlikte barındırma platformları, Metaverse'de sınırlar belirliyor ve emniyet ve güvenlik için kurallar uyguluyor. Metaverse araştırmalarındaki potansiyel bir yasal zorluk, platformlardaki yarı adli sistemlerdir. Platformlar, verilerin açıklanıp açıklanmayacağı veya platformda yaptırımın uygulanıp uygulanmayacağı konusunda bir anlaşmazlık olması durumunda, kişi ve kuruluşların kendi durumlarını platform tarafından seçilen bir grup "uluslararası uzmana" sunmalarını talep edebilir.
- Platform müdahalesinin ötesinde, bazı eylemlerin ciddi zarara, mali kayba yol açabileceği veya gerçek dünyada sonuçlara yol açabileceği ve kolluk kuvvetlerine rapor verilmesini gerektiren senaryolar vardır. Bu nedenle, Metaverse'de veya Metaverse aracılığıyla kaynaklanan zararları ele almak için bu eşik tabanlı sistemi tasarlamak önemlidir. Zarara tepki için bir eşik oluşturmanın yanı sıra, sağlam bir raporlama mekanizması da gerekli olacaktır.

Uluslararası Kolluk Kuvvetleri İşbirliği

Metaverse'den kaynaklanan küresel tehditler ve zararlar karşısında, ortaya çıkan bu zorlukların üstesinden gelme çabalarının temelinde uluslararası kolluk kuvvetleri işbirliği yer alıyor. Bu nedenle, tasarım gereği güvenli (tasarım gereği güvenlik ve tasarım gereği gizlilik gibi hususlar dahil) bir Metaverse oluştururken küresel kolluk kuvvetlerinin perspektiflerini yansıtmak önemlidir. Örneğin, metasuç soruşturmaları için ilgili verilere zamanında erişime izin verilmesi, gizlilik ve diğer temel hakların sağlanması yararlı olacaktır. Metaverse'deki suçlar sıklıkla birden fazla sanal ortamda ve birden fazla yargı bölgesinde işlendiğinden, farklı yasa ve düzenlemelerin uyumlu hale getirilmesi de faydalı olacaktır. Bu çabalar, sanal dünyayı güvenli ve emniyetli tutmak için kolluk kuvvetlerinin etkili müdahalesini ve sınır ötesi işbirliğini mümkün kılacaktır.

Avatarların Hukuki Durumu ve Sorumluluğu

Soruna bir karmaşıklık katmanı ekleyen yapay zeka tabanlı avatarlar, suç faaliyetlerinin karmaşıklığını, miktarını ve hızını artırmak amacıyla Metaverse'deki suçlarda kullanılabilir. Kimlik yapısına ilişkin önceki bölümde de belirtildiği gibi, bu durumda özerk bir tüzel kişilik söz konusudur. Anahtar soru, yapay zeka tabanlı avatarı kimin veya hangi varlığın kontrol ettiği olacaktır. Bir adamın yapay zekayı çocuk cinsel istismarına yönelik materyaller oluşturmak için kullandığı gerekçesiyle iki buçuk yıl hapis cezasına çarptırıldığı yakın tarihli bir davadan ders çıkarılabilir. Bu karar, gerçek çocuklara veya reşit olmayanlara benzeyecek kadar gerçekçi, sanal insanları içeren materyallerin yasa dışı olduğunu doğruladı. Düzenleyici çerçeveler güncel olmalı ve yapay zeka tabanlı avatarlar tarafından işlenen veya kolaylaştırılan suçlarla ilgili bu sorumluluk konularını ele almaya hazır olmalıdır.

Birlikte Çalışılabilirlik

- Birlikte çalışabilirlik, metaversein tüm potansiyelini ortaya çıkarabilecek çok önemli ancak karmaşık bir konudur. Dünya Ekonomik Forumu'na göre, birden fazla sanal dünyada ekonomiyi, avatarları ve sistemleri birleştirmek için çok çeşitli teknik, kullanım ve yargısal hususları kapsamaktadır. Bir kez başarıldığında kesintisiz ve sorunsuz bir deneyim sunabilir ve bu da kitlesel benimsenme için ağ etkilerine neden olur.
- Farklı üç boyutlu sanal dünyalardan oluşan birlikte çalışabilir bir ağ sağlamak için ekosistemin varlık sahipliği, kimlik, veri gizliliği, fikri mülkiyet, demografik kapsayıcılık, veri yönetimi ve yetki alanındaki zorluklarla ilgili çeşitli konuları ele alması gerekecektir. Metaverse'deki teknik birlikte çalışabilirliği yansıtmak, yasal veya düzenleyici birlikte çalışabilirlik için de gereklidir.
- Birden fazla metaversede kişi başına benzersiz bir dijital kimliğe sahip olmak da düşünülebilir. Tüm bu sorunların küresel kolluk kuvvetleri topluluğu için sonuçları olduğundan, kolluk kuvvetlerinin etkili müdahalesine yönelik ilerlemeyi takip etmek için gelişmelerin yakından izlenmesi büyük önem taşımaktadır.

Güvenlik ve Emniyet

- Metaverse çeşitli siber saldırılara karşı savunmasız olabilir. Örneğin, yanlış bilgilendirme ve dezenformasyon da dahil olmak üzere zararlı içeriklerin yayılması için kullanılabilir. Bu, üç boyutlu, sürükleyici, kalıcı ve kenarlıksız yapısı nedeniyle bu tür içeriğin etkilerini arttırması nedeniyle özellikle zarar verici olabilir. Bu, fiziksel dünyada doğrudan sonuçları olabilecek ciddi gizlilik ve güvenlik ihlallerine yol açabilir. Bu nedenle, bu endişeleri gidermek için güçlü siber güvenlik önlemlerinin uygulanması gerekmektedir. Meta Suçlarla ilgili Bölüm II'de

özetlenen suçlara karşı savunmasız olabilecek metaversedeki çocukları daha iyi korumak için platformlar ve hizmet sağlayıcılar, çocuk güvenlik kilitleri ve filtreleri gibi koruma önlemlerini uygulamayı düşünmelidir. Güvenlikle ilgili diğer sorunlar, VR'da akşamdan kalmalık gibi sağlık sorunlarını içerebilir.

- Ayrıca, kullanıcı gizliliğinin etkili bir şekilde korunması için sağlam ve uyarlanabilir veri koruma önlemleri ve çerçevelerinin oluşturulması da önemlidir. Metaverse Güvenlik Haftası 2023'te vurgulandığı gibi, önemli miktarda veri toplama ve işleme özelliği göz önüne alındığında, özellikle yapay zeka destekli Metaverse'de gizlilik riskleri artabilir. Bu nedenle çevik bir veri koruma çerçevesi, kullanıcıları Metaverse'de yapay zeka tarafından işlenen verilerin olası kötüye kullanımına karşı korumak için çok önemli olacaktır. Bu aynı zamanda çeşitli gizlilik ve güvenlik kontrolleriyle düzenleyici çabalara ve girişimlere yardımcı olabilir ve bunları güçlendirebilir.
- Göz önünde bulundurulması gereken bir diğer husus, deneyimlerin ve kaynaklarının nasıl tanımlanabileceği ve atfedilebileceğidir. Mevcut İnternet veya sosyal medyadaki (örneğin, URL) bir bilgi kaynağına atıfta bulunma yöntemleri Metaverse'de işe yaramayabileceğinden, Metaverse'deki kaynakları tanımlama süreci hala belirsizdir. Belirli bir deneyimin birden fazla örneğinin de mümkün olduğu göz önüne alındığında, bu çokluk, hangi belirli örneğin kaynak olarak hizmet ettiğini belirlemede zorluklar yaratabilir.

Etkin Yönetim

- **Suçlulaştırma**

Metaverse'deki kötü niyetli davranışların ve yasa dışı faaliyetlerin suç sayılması, yerleşik yasaların olmasını ve bu tür eylemlerin suç teşkil eden davranışlar olarak tanınmasını gerektirir. Metaverse'deki gelecekteki suçların tümü geleneksel suçların tanımlarına uymadığından, bu, net tanımların oluşturulmasını gerektirir. Örneğin hibrit (fiziksel-sanal) etkileşimleri içeren suçlar, yeni veya revize edilmiş tanımlar gerektirebilir. Ancak, tanımın daha fazla belirsizliği daha fazla çelişkiye ve hukuki sonuçlarda öngörülemezliğe yol açabileceğinden, belirsiz ve geniş suç tanımlarından kaçınmak önemlidir. Bu nedenle suç teşkil eden davranışların bu doğrultuda cezalandırılmasını sağlayacak net tanımların oluşturulmasına ihtiyaç vardır. Ayrıca kolluk kuvvetlerinin Metaverse ortamındaki gerçek ve gerçek gerçekleri değerlendirebilmesinin yanı sıra ilgili cezai sorumluluk yaşını uygulayabilmesi de önemli olacaktır.

- **Gelecek Odaklı Politika**

Metaverse'i düzenlemek için benimsenen herhangi bir politikanın veya yasal çerçevenin geleceğe yönelik olması çok önemlidir. Metaverse platformları ve teknolojileri gelişmeye devam edecek ve hayal edilemeyecek şekillerde değişebilir. Geleceğe hazır politikalar ve yasalar kapsamlı bir strateji gerektirir. Gelecekteki bilinmeyen teknolojilere kolayca

uygulanabilecek, teknolojiden bağımsız terminolojinin kullanılması gibi yasa veya politika tasarım teknikleri yardımcı olabilir. Politikaların ve yasaların sistematik ve düzenli olarak gözden geçirilmesi, bunların etkililiğinin değerlendirilmesine ve güncel tutulmasına yardımcı olabilir. Bu incelemeler, ilgili kamu kurumlarının (örneğin, düzenleyiciler, kolluk kuvvetleri) ve diğer paydaşların (örneğin, özel sektör ve sivil toplum) Metaverse teknolojilerinin gelişimi ve ilgili suç eğilimleri hakkında periyodik raporlar üretmeleri için yasal gerekliliklerle desteklenebilir.

SONUÇ

Teknolojik gelişmelerin ve sürekli yeniliklerin damgasını vurduğu, hızla gelişen bir dünyada, kolluk kuvvetlerinin çevik ve dirençli kalması hayati önem taşımaktadır. Bu, yeni gelişmelerin sürekli izlenmesini ve bu değişikliklerin etkisinin analiz edilmesini gerektirir. Bu çabanın bir parçası olarak, bu Teknik Rapor, Metaverse'in çok yönlü yönlerine ilişkin önemli bilgiler sunmaktadır.

Tasarım gereği güvenli bir Metaverse'e katkıda bulunmak amacıyla bu makale, INTERPOL Metaverse Uzman Grubu'ndan gelen girdilere dayanarak, Metaverse'nin çeşitli boyutlarının kolluk kuvvetleri perspektifinden kapsamlı bir analizini sunmaktadır. Özellikle kapsamlı eğitim ve diğer kullanım senaryoları alanlarında, Metaverse'nin kolluk kuvvetleri için etkili bir araç olarak oynadığı role ilişkin farkındalığı artırır. Aynı zamanda çeşitli Metasuç türlerinin bir tipolojisini de sunar.

Metaverse'deki adli tıp ve soruşturmalar açısından, bu makale, son noktalar, sunucular, motorlar ve platformların yanı sıra sanal varlık analitiği de dahil olmak üzere, kanıtlara erişirken ve ortaya çıkarırken dikkate alınması gereken birkaç temel unsurun ana hatlarını çiziyor. Karmaşık yönetişim konularını ele almak için mevcut ulusal ve uluslararası yasaların uygulanmasının değerlendirilmesi, boşlukları azaltmak için düzenli politika incelemeleri yapılması ve geleceğe yönelik politikaların tasarlanması tavsiye edilir.

Metaverse'nin birden fazla yetki alanını, boyutu ve kuruluşu kapsadığının bilincinde olarak, çok paydaşlı katılımları ve sınır ötesi işbirliğini içeren bütünsel bir yaklaşım, Metasuça etkili bir kolluk kuvveti müdahalesi için çok önemlidir. INTERPOL, güvenli ve emniyetli bir Metaverse oluşturmaya yardımcı olmak için dünya çapındaki çeşitli paydaşlarla bu diyaloğu sürdürmeye hazırdır. INTERPOL, küresel emniyet teşkilatına destek olarak, gelecekteki dünyamızı koruma çabalarının ön saflarında yer almaya devam edecektir.