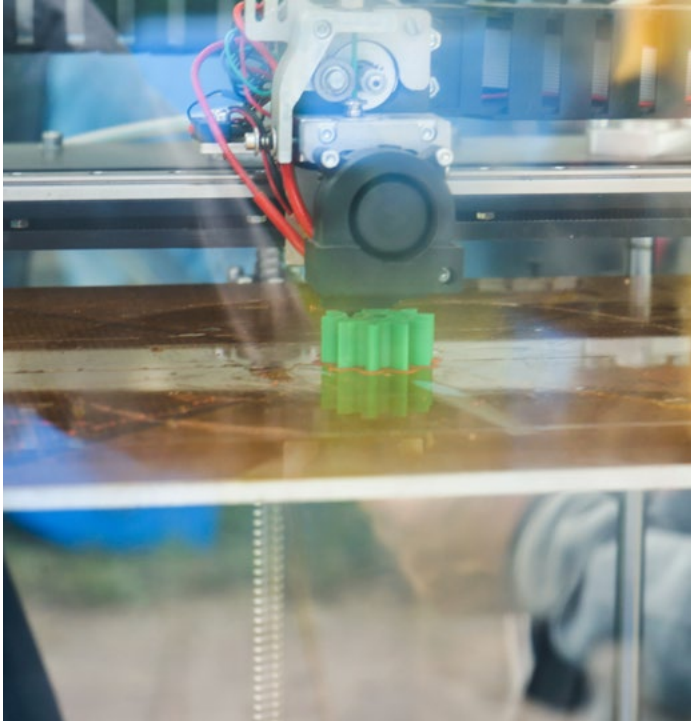
thinktech
STM Teknolojik Düşünce Merkezi



3D Baskı ve Güvenlik Sorunları

Hızlı prototipleme ve üç boyutlu (3D) baskı yöntemi olarak uzunca bir zamandır kullanılan teknolojinin endüstrileşen hali olan katmanlı imalat, kısa ve uzun vadede potansiyel güvenlik etkileriyle yerel ve uluslararası alanda gelişmekte olan bir teknolojidir.

Katmanlı imalat teknolojisi ilk olarak 1980'li yıllarda konuşulmaya başlandı. Bu çığır açan teknoloji, ana üretim süreçlerini dönüştürmek için basit prototip oluşturma ve amatör tasarım çabalarının ötesine hızla yayıldı. Hâlihazırda 3D yazıcılar, tıbbi cihazlardan, otomobil parçalarına hatta karmaşık havacılık sanayine kadar çok sayıda ürünün üretimine yardımcı olmaktadır. Bugün dünyanın dört bir yanındaki teknoloji meraklıları 3D baskının artan önemini takdir ediyor. 3D teknolojisiyle üretim ya da diğer adıyla katmanlı üretim geleneksel üretimden farklı olarak malzeme kullanımında atık yaratmadığı için verimlilik bakımından çok ciddi faydalar sağlıyor. Ayrıca 3D yazıcıların fiyatlarının düşmesiyle herkesi evinden üretim yapar hale dönüştürerek üretimin tabana yayılmasını sağlıyor. İnternetin olanaklarıyla herhangi bir ürünün tasarımını çoğu zaman ücretsiz elde etmek ve bunu üretimde kullanmak da mümkün ve bu trend de hızla yayılıyor. Kuşkusuz 3D teknolojisinin vaatleri ve sosyal faydaları çok önemli ancak her dönüşüm teknolojisinde olduğu gibi, zarar verme potansiyeli de oldukça büyük. Yeni araştırmalar 3D baskı ile ürünlerin, tespit edilemez kusurlarla taklitlerini yapmak için değiştirilebileceğini gösteriyor. Örnek vermek gerekirse, biyometri alanında 3D yazıcılarla insanların parmak izlerini kopyalarak birçok cihaza giriş yapılabileceği ve/veya kriminal suçlarda suçsuz kişilerin parmak izleri suç mahalinde kullanılarak güvenlik ve mahremiyet gibi zafiyetlere yol açabileceği bilinmektedir.

Katmanlı Üretim ve Gelecekteki Güvenlik Tehditleri

Katmanlı imalat kendi başına bir tehdit oluşturmaz. Tam tersi toplum için büyük faydalar sağlayabilir. Bununla birlikte bu faydalar kötü sonuçlar için de kullanılabilir. Üreticiler için katmanlı imalatı değerli kılan özellikler kötü niyetlileri de kendine çekebilir.

3D baskı teknolojisi, imalat işletmelerine çeşitli faydalar sunarken, bu süreç aynı zamanda yanlış kullanım potansiyelini de barındırır. Hacker'lar, ticari bilgisayarların ve ticari mülkiyetin çalınması için tahrip edici virüslerin bulaşmasını sağlayarak iş bilgisayarlarını aksatmanın yollarını bulmuşlardır. Benzer şekilde, suçluların 3D yazdırma protokollerini ve dijital tasarım dosyalarını bozması için çok sayıda yol bulunuyor.

ABD'nin ünlü think tank kuruluşu RAND Corporation, 2040 yılına ilişkin katmanlı imalat teknolojisinin güvenlik zorluklarını inceleyerek raporlaştırdı. "Additive Manufacturing in 2040" adlı rapor, 3D yazıcıların değiştirici potansiyeline artan ilgi göz önüne alındığında, özellikle bu teknolojinin 2040 yılında güvenlik odaklı olası olumsuz

etkilerini araştırıyor. RAND'ın araştırma ekibinin mevcut literatürü gözden geçirmesiyle oluşturulan rapor, paydaşlar ve konunun uzmanlarıyla röportajlar ve teknoloji/güvenlik uzmanlarıyla yapılan atölye çalışmalarını kapsıyor[1].

Muhtemel geleceği daha iyi tahmin etmek için katmanlı imalat teknolojisinin en çok sonuç veren etkilerine odaklanan raporda 2040 yılında tehdit ortamını araştırmak için iki temel soru soruldu. Bu sorular şunlardı:

1. 2040 için yapılan gelecek tahminlerinin kişisel güvenlik, iç istikrar ve uluslararası düzen açısından farklı etkileri nelerdir?
2. Bugün kanun koyucular gelecek tahminlerinin yönünü şekillendirmek için hangi stratejileri kullanabilir?

2017 Mart ve Ağustos ayları arasında 11 görüşme gerçekleştirildi. 2040 yılında kritik güvenlik zorluklarını inceleyen çalışmada, iki kapsamlı güvenlik tehdidi ortaya çıktı: Bunlar silahların yayılması ve ekonomik güvensizlikti.

Sonuç olarak, 3D yazıcıların çoğalmasının, hem avantajlar hem riskler getireceği ve risklerin tam olarak önlenemeyeceği, toplumun ve kanun koyucuların bunu kabul etmesi gerektiği tartışıldı.

Deloitte'un "3D Opportunity for Adversaries" adlı raporunda ise katmanlı imalat tarafından doğrudan geliştirilebilen tehdit alanları incelendiğinde, bunların beş başlıkta toplandığı görülüyor[2]:

- **Ev Yapımı Ateşli Silahlar:** İnternetten indirilen planlarla amatör seviyede katmanlı imalat makinelerinde yapılan geliştirilmiş plastik ateşli silahlar.
- **Taklitler**: Güvenilir bir tedarikçinin güvenilir bir ürününü taklit etmek için tasarlanmış ve üretilmiş ürünler veya bileşenler. Ürünler, taklit tüketim mallarından kredi kartı tarayıcılarına hatta askeri donanımlar için sahte parçalara kadar çeşitlilik gösterebilir.
- **Uyarlanmış Patlayıcı Aygıtlar:** Gelenekselin dışındaki patlayıcı aygıtlar.
- **Gelişmiş Teknoloji/Silahlar:** Jet motoru teknolojisi, füze teknolojisi ve gelişmiş patlayıcılar gibi genellikle ithalatı kontrollü teknolojiler.
- **CBRNE Tehditleri:** Kimyasal, biyolojik, radyolojik, nükleer ve patlayıcı (CBRNE) tehditlerin üretiminin yanı sıra silahlandırılmasını hızlandırma araçları.

Deloitte'un raporuna göre, potansiyel tehditlerin çeşitliliği ve katmanlı imalatın kullanılabileceği yollara karşı tek bir yaklaşımla korunabilmek anlamlı değildir. Katmanlı imalatın tehdit edici kullanımlarına karşı alınacak önlemler, ihracat yönetmeliklerinden suçluların gözetimine, istihbarat değerlendirmelerinden dijital dosyaların düzenlenmesine ya da makinelerin satışlarının izlenmesi yollarına kadar her yaklaşımı kapsayabilir. Bu çabaların etkinliği nihayetinde bu önlemlerin koordinasyonunda yatmaktadır.

Buna göre katmanlı imalatın olumsuz kullanımlarına karşı korunmak için aşağıdaki adımlar dikkate alınmalıdır:

1. Uluslararası bir eylem topluluğu oluşturma: Geleneksel sınırlar karşısında hızla işbirliği yapmak için hükümet, sanayi ve uluslararası kuruluşlar arasında mekanizmalar oluşturmak.
2. Ortak bir endüstri ve uluslararası politikaya yönelmek: Endüstrinin, uluslararası aktörlerin ve hükümetlerin katıldığı tek ve açıkça belirlenmiş bir politikaya doğru çalışmaya başlamak.

Katmanlı İmalat ve Küresel Tehditler

Katmanlı imalatın gelişimi ve yayılımı silahların çoğalmasını önemli ölçüde hızlandırarak uluslararası çatışmalar, şiddet yanlısı radikaller ve suç oranları üzerinde dramatik etkilere sebep olabilir. Ateşli silahlar ve drone'lar gibi riskli ürünlerin satış noktasında devlet kontrolü imkânı ortadan kalkabilir.

1 https://www.rand.org/pubs/perspectives/PE283.html
2 https://www2.deloitte.com/insights/us/en/focus/3d-opportunity/national-security-implications-of-additive-manufacturing.html

Devlet egemenliği, gücün tekelliğine dayanır ve ateşli silahları düzenleme kapasitesine sahiptir. 3D yazıcılar bu kontrolü zayıflatarak vatandaşlara ölümcül silahlarla diğer şiddet araçlarına daha fazla erişim imkânı sunuyor. Protestoculardan suç şebekesi üyelerine kadar herkesin silahları hızla üretme yeteneğine sahip olmasıyla ülkeler toplum kontrolünde artan tehditlerle karşı karşıya gelecek.

Amerika Birleşik Devletleri gibi yarı otomatik silahların yaygın olarak erişilebilir olduğu ülkelerde 3D yazıcılar toplu katliam riskini artırabilir. İnternette bulunan geniş kaynaklardan istediği silahı yazdıracak tasarıma ulaşabilen biri, daha erişilebilir silahlar yaparak ölümcül saldırıların potansiyelini de arttırabilir. Ayrıca, teröristlerin internet üzerinden yeni ve daha tehlikeli olan silahların yazdırılabilir hazır tasarımlarına erişim imkânlarının olması; okullar, hükümet binaları, havaalanları gibi konumlarda silahları hızlı bir şekilde yapmalarını daha kolay hale getirecek. Bu güvenli alanlar bile, olası bir saldırganın 3D yazıcı ve internete erişebilmesi durumunda iç tehditlere karşı savunmasız kalabilir.

ABD ordusu teknolojiye yaptığı yatırımlarla dikkat çekiyor. Çin'in de savunma amaçlı 3D yazıcılarla yakından ilgilendiği biliniyor. Diğer taraftan, katmanlı imalat Kuzey Kore gibi uluslararası toplumdan kendini çekmiş devletlerin hayatta kalmasını ve yükselişini dolaylı olarak destekleyebilir. Nispeten istikrarlı devletlerde bile 3D yazıcılarla yapılan silah ve diğer ürünlerin karaborsayı doldurmasının, suç ağlarına yeni bir gelir akışı kazandırması bekleniyor.

3D yazıcıların tehdidi bu devletler arası dinamiklerin çok ötesine geçiyor. Şiddet eğilimli organizasyonlar, günümüzün en büyük güvenlik tehditlerinden bazıları ve 3D yazıcıların çoğalmasıyla daha da tehlikeli olmaları bekleniyor. Şiddet eğilimli organizasyonların büyümelerini takip etmek gittikçe zorlaşacaktır çünkü bunların tehdit değerlendirmeleri ve diğer güvenlik analizleri genellikle silah satışları ve diğer malzeme teminleriyle ilgili bilgilere dayanır. Bu akışları izlemek, kolluk güçleri ve istihbarat ajanslarına şiddet eğilimli organizasyonların tehditlerini değerlendirmek ve ağlarını belirlemek için kritik fırsatlar sunuyor.

Bu organizasyonlar 3D yazıcıyla her istediklerini üretebilirlerse geç kalmadan faaliyetlerini tespit etmek veya bozmak çok daha zor olacak. Kaçakçılık ve yasadışı sevkiyatların azalmasıyla ortaya çıkacak ani bir saldırı, bu organizasyonların daha gelişmiş yeni özellikler edindiklerinin ilk işareti olabilir. 3D yazıcılarla bu tür saldırılar daha ölümcül ve yaygın olabilir.

Kamusal alanlar her zaman savunmasız olsa da, özel alanlar için (stadyumlar, ofis binaları gibi...) çeşitli önlemler alınarak en azından silahlı saldırılar gibi şiddet olaylarının azaltılması olası. Ama 3D yazıcılar güvenli alanları bile tehdit etme potansiyeline sahip. Olası bir saldırgan havaalanları veya diğer güvenli tesislerin el tarayıcıları ve metal dedektörlerinden geçtikten sonra, sadece internet bağlantısı ve 3D yazdırma noktasıyla büyük bir kargaşaya neden olabilir.

Katmanlı İmalat ve Siber Tehditler

3D baskı teknolojisinin popülaritesindeki artış ve buna paralel olarak sundukları ile, günümüzde heyecan verici fırsatlarla birçok sektörde işletmelere hizmet vermektedir. Bununla birlikte, bu alanın hızla gelişen etkileyici faydaları ile birlikte siber güvenlik riski de artmaktadır.

Rutgers Üniversitesinden Todd B. Bates yazdığı bir makalede, "3D baskılı nesneler ve parçalar dünyanın dört bir yanındaki kritik altyapılarda kullanılıyor ve siber saldırılar sağlık hizmetleri, ulaşım, robotlar, havacılık ve uzay alanlarında risklere neden olabilir" diyor[3].

Siber güvenlik tehditlerinin takibi diğer tehditlere göre daha zor ve karmaşıktır. Katmanlı imalat ve siber dünya arasındaki potansiyel ilişkiyi düşünürsek, 2017 yılındaki küçük ölçekli ve yabancı siber saldırıların fiziksel olmayan olaylar olduğunu görüyoruz (örneğin bir çevrimiçi satıcının hassas müşteri bilgilerini hack'lemek). Saldırıya

3 https://www.techrepublic.com/article/3d-printing-security-risks-threaten-the-publics-health-and-safety/

uğrayanın bilgileri daha sonra kâr amacıyla satılır veya dolandırıcılık için kullanılırdı. Bilgisayar korsanları artık kişisel veya finansal bilgileri çalmanın dışında hassas teknolojilerin tasarımlarına da erişebilir. Katmanlı imalat ile siber savaşın çıkar payları artabilir.

New York merkezli bir akademik araştırma ekibi, bilgisayar korsanlarının, ürün kalitesini etkileyebilecek tasarım değişiklikleri yapabileceği sonucuna vardı. Örneğin, bazı durumlarda, bir ürünün 3D baskı sırasında tasarımına yapılacak müdahale, belirli bir amaç için gücünü ve faydasını etkileyebilir[4].

Bir 3D yazıcıya erişim sayesinde, bir bilgisayar korsanı ev yapımı bir jammer teknolojisiyle gözlenmeyi engelleyerek siber saldırı tehdidini arttırabilir. Bu tehdit özellikle hacker'ların bir yazıcıya sızarak kritik parçaların tasarımlarına kusurlar eklemesi veya dijital tasarımları bozmasıyla daha ciddileşebilir (uçak gövdesi veya otonom bir araba tasarımı gibi). Dijital tasarımlar daha fazla somutlaştıkça bu saldırıların dijital alanın ötesinde gerçek dünyada daha fazla sonuçları olacak, fiziksel ve sanal tehditler arasındaki sınır da bulanıklaşacak.

Katmanlı İmalatın Ekonomik Etkileri

3D yazıcılar, silahların çoğalması ve siber savaşlarla birlikte, ekonomileri ve uluslararası piyasaları bozma potansiyeline de sahip. Sanayi Devrimi'nin 18. ve 19. yüzyıllardaki etkileri gibi katmanlı imalat, özelleştirilebilir ve karmaşık ürünlerin kullanımını yaygınlaştırarak geleneksel ekonomilerin ölçeğini geliştirebilir. Aynı zamanda, devlet dışı güçlerin, önceden sadece gelişmiş devleterin sahip olduğu uzmanlık ve endüstriyel kapasite gerektiren ürün gelişimlerine ulaşmasını sağlayabilir. Halen gelecekte ne tip ve ne kadar sayıda ürünün üretileceği belirsizken 3D yazıcıların çoğalmasıyla hammedelere kolay erişim ve dijital planların serbestleşmesi küresel ekonomiyi, uluslararası güvenliği ve toplumu derinden değiştirebilir.

3D yazıcıları kullanan firmalar, geleneksel imalatta çalışan çok sayıda vasıfsız çalışana karşılık genellikle yüksek eğitimli ve yetenekli çalışanlara ihtiyaç duymakta. Bir uzmana göre, "Artık bir milyon makinede çalışan insanlara ihtiyaç duyulmayacağından ülkelerde daha düşük endüstriyel üretim ve daha düşük emek katılımı olacak." Yani teknoloji ilerledikçe, aynı miktarda çıktı üretmek için daha az çalışan yeterli olabilir; dolayısıyla bir kutunun içine bir fabrikayı sığdırabilirsiniz[5].

Gelişmiş ve gelişmekte olan ülkelerde 3D yazıcıların etkisiyle işsizliğin, izolasyonun, yabancılaşmanın ve düşük vasıflı işçi oluşumunun şiddetlenmesi ekonomik eşitsizliği arttırarak toplumsal huzursuzluğa yol açabilir. Toplumlarda işssizliğin büyümesinin güvenlik etkileri önemli olabilir. Gelişmekte olan ülkelerin artan ekonomik bağımsızlığıysa mevcut dünya düzenini hem olumlu hem de olumsuz sonuçlarla değiştirebilir. Az gelişmiş ülkeler kapsamlı üretim yeteneklerine sahip gelişmiş ülkelere ihracat yapmak yerine kendilerine çok daha küçük sermaye yatırımları yapabilirler. Bu, birçok alanda yardım ihtiyacını azaltabilir ancak diğer alanlarda ekonomik eşitsizlikleri de arttırabilir.

Wohlers Associates'e göre, küresel 3D baskı pazarının 2020 yılına kadar 21 milyar dolara ulaşması bekleniyor. Katmanlı İmalatın büyümesinin, küresel ticareti ise 2060 yılına kadar yüzde 25 oranında azaltabileceği öngörülüyor[6].

Etki Azaltma Stratejileri ve Politikası

3D yazıcıların donanım, yazılım ve hammaddelerinin evrilmesi ve düzenlenmesiyle gelecekteki tehditlerin risk ve sonuçlarının ne olacağı göreceli. 3D yazıcıların potansiyel tehditlerini tam olarak anlayabilmek ve etkisini azaltmak için tehdit önleme, zarar hafifletme, ilişkilendirme ve sorumluluk gibi stratejilerin ele alınması gerekiyor.

4 https://bdtechtalks.com/2017/07/05/the-cybersecurity-risks-of-3d-printing/
5 https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE283/RAND_PE283.pdf
6 http://www.applerubber.com/blog/5-of-the-biggest-challenges-facing-manufacturers-in-3d-printing/

a) Tehdit Önleme

Katmanlı imalatta riskler açısından ilk ve en iyi çözüm, bozulmayı veya saldırıyı önlemektir. 3D yazıcı firmaları dünyaya yayılmış durumda. Bu nedenle tek taraflı herhangi bir önlem oldukça etkisiz olacaktır. Nükleer teknolojinin ilk yıllarında, Amerika Birleşik Devletleri etkili bir şekilde tek taraflı önlemlerle gelişimini ve çoğalmasını sınırlamak için çalışmalar yaptı. Ancak bir teknoloji daha geniş kullanıma veya geliştirmeye ulaştığında (örneğin hipersonik silahlar), daha sonrasında çok taraflı çabalar (örneğin ortak ihracat kontrolleri anlaşmaları) gereklidir.

Silahların yayılmasını önlemek için gerçekten alınabilecek birkaç önlem var. Donanım açısından yerel yönetmelikler, özgeçmiş kontrolleri ve diğer kısıtlamalar ile yazıcıların satın alınmasını sınırlayabilir. Perakende seviyesindeki bu kontrollerle 3D yazıcıların şiddet eğilimli organizasyonlara yayılmasını önlemek veya en azından süreci yavaşlatmak mümkün. Ancak, bu kontroller 3D yazıcıların kendi kendini çoğaltma yetenekleri daha da geliştikçe etkisiz hale gelecektir. Malzeme kontrollerine odaklanılırsa tehdit önleme daha da etkili olacaktır. Nadir veya tehlikeli hammaddeler ve düzenleyici maddelerin sınırlandırılmasıyla en azından en yıkıcı silahların (örneğin nükleer veya kirli bombalar) bazılarının şiddet eğilimli organizasyonlarca kolayca erişebilir olması engellenebilir.

b) Zarar Hafifletme

Önleyici tedbirler 3D yazıcıların olumsuz sonuçlarının yayılmasını durdurmayacaktır. Bu nedenle, kanun düzenleyicilerin gelecekte özellikle zarar hafifletmeye yönelik tedbirlere odaklanması da gerekir.

Donanımsal olarak yeni veya daha gelişmiş cihazlar için internetten yazıcının kayıt edilmesi kontrol açısından bir olasılık olabilir. Güvenlik önlemleri, kayıt dışı cihazlar için işlevselliği sınırlayabilir. Düzenli çevrimiçi güncellemelerin yapılmadığı durumlarda cihazların çalışamaz hale gelmesi veya bazı işlevleri kaybetmesi önlem olarak uygulanabilir.

c) İlişkilendirme ve Sorumluluk

Ne yazık ki, bazı durumlarda zarar hafifletme bile uygulanabilir olmayacaktır. Devlet makamları açısından, bir saldırıyı engelleyememe durumunda, ilişkilendirme ve sorumluluk başvurulacak son yöntem olmaya devam ediyor. 3D yazıcı bağlantılı bir saldırı, kolluk kuvvetlerini faillerin takibi ve sorumluların tespiti çabalarında yeni zorluklarla karşı karşıya getirecek. Kanun düzenleyiciler bu süreci desteklemek için yeni yöntemler düşünmelidir. Örneğin, düzenleyici standartlar, yazıcıların ürünlerine benzersiz bir kimlik bilgisi kodlamasını gerektirebilir böylece ilişkilendirme işlemi kolaylaşır.

Bu ilişkilendirme teknolojilerinin çoğu halen erken gelişim aşamasında bulunuyor ve fizibilitesi belirsiz. Ancak tehdit önleme ve zarar hafifletme aşamalarındaki zorluklar, ilişkilendirme ve sorumluluğu kanun düzenleyiciler açısından yatırım yapılabilecek umut verici alanlar haline getiriyor. Bugün verilen kararların, gelecekte karşılaşılacak fırsatları ve tehditleri şekillendirme gücü ise unutulmamalı...