Sürdürülebilir Mühendislik Uygulamaları veTeknolojik Gelişmeler Dergisi
Journal of Sustainable Engineering Applications and Technological Developments
2024, 7(2): 104-113

Siber-Biyosuç: Sentetik Biyoloji ve Geleceğin Suçları

Cyber-Biocide: Synthetic Biology and Crimes of The Future

Fatma Altıntaş[1*], Atakan Konukbay[2], Ahmet Koluman[3]

[1*] Pamukkale University, Department of Biomedical Engineering, Denizli, Turkey
[2] CBRN Product Management, HAVELSAN, Ankara, Turkey
[3] Pamukkale University, Department of Biomedical Engineering, Denizli, Turkey

ÖZET

Bu makale, sentetik biyoloji ve siber suçların kesişimini ele alarak geleceğin suç potansiyellerini analiz etmektedir. Sentetik biyoloji, organizmaların yeni yeteneklerle yeniden tasarlanmasını içeren bir alandır ve hızla gelişen teknolojilerin yaygınlaşmasıyla yeni suç fırsatları doğurmaktadır. Siber-biyosuç, internet bağlantılı laboratuvarlar ve biyoteknoloji sistemlerinin kötü niyetli kullanımını içerir. Bu makale, biyolojik ayrımcılık, biyolojik kötü amaçlı yazılım, gen düzenleme ve evde yasadışı uyuşturucu üretimi gibi potansiyel suç örneklerini ele almakta ve önleme stratejileri üzerinde durmaktadır. Yasal düzenlemeler, uluslararası iş birliği, eğitim ve teknolojik güvenlik, gelecekteki suçların önlenmesinde kritik öneme sahiptir.

Anahtar Kelimeler: Sentetik biyoloji, Siber-biyosuç, Yasal düzenlemeler, Uluslararası iş birliği, Teknolojik güvenlik

ABSTRACT

This article, analyzes future crime potentials by addressing the intersection of synthetic biology and cybercrime. Synthetic biology is a field that involves the re-engineering of organisms with new capabilities, and the proliferation of rapidly developing technologies opens up new criminal opportunities. Cyber-biocrime involves the malicious use of internet-connected laboratories and biotechnology systems. This article discusses examples of potential crimes such as biological discrimination, biological malware, gene editing and illicit drug production at home, and focuses on prevention strategies. Legislation, international cooperation, education and technological security are critical to preventing future crimes.

Keywords: Synthetic biology, Cyber-biocide, Legal regulations, International cooperation, Technological security

Başvuru: 25.07.2024 Revizyon Talebi: 16.08.2024 Kabul: 24.08.2024
Doi: 10.51764/smutgd.1522515

[1]*Sorumlu yazar: Pamukkale University, Faculty of Technology, Denizli, Turkey ; E-mail: fatma.altintas53@gmail.com; ORCID: 0000-0002-7871-1967
[2] E-mail: akonukbay@havelsan.com.tr ; ORCID: 0000-0003-2404-0253
[3] E-mail: akoluman@pau.edu.tr ; ORCID: 0000-0001-5308-8884

1. GİRİŞ

Sentetik biyoloji, organizmaların yeniden tasarlanması ve yeni yeteneklere dönüştürülmesi sürecini içeren disiplinlerarası bir alan olarak tanımlanmaktadır. Bu alandaki hızlı teknolojik ilerlemeler, tıp, üretim ve tarım gibi pek çok sektörde çözümler sunma potansiyeline sahip olmakla birlikte, aynı zamanda siber suçlar gibi yeni riskleri de beraberinde getirmektedir (Elgabryvd., 2020; Murch vd., 2018). Biyolojik malzemelerin kullanılmasıyla gerçekleştirilen fiziksel süreçlerin, istenmeyen ve tehlikeli biyolojik sonuçlara yol açabileceği gerçeği göz önünde bulundurulmalıdır. Bu nedenle, sentetik biyoloji alanındaki ilerlemeler, bir yandan yararlı ve olumlu sonuçlar sunarken, diğer yandan da potansiyel suç fırsatları oluşturabileceği bilinciyle ele alınmalıdır (Mueller, 2021). Dünya genelindeki araştırmacılar ve şirketler, sentetik biyolojinin potansiyelini kullanarak sağlık sorunlarına çözümler bulma çabasındadır. Bu durum, sentetik biyolojinin daha önce sadece araştırma kurumlarında sınırlı kalan bir alandan, yaygın bir şekilde erişilebilir ve maliyeti düşük bir alana dönüşmesine yol açmıştır. Örneğin, insan genomunun dizilenmesi için önceden yüksek maliyetler gerektiren bir işlem, günümüzde daha uygun fiyatlı hale gelmiştir (NHGRI,2021).

Sentetik biyolojinin hızla yayılımı ve düşen maliyeti, aynı zamanda siber suçlar ve biyoteknolojinin kötüye kullanımı için de kapılar açmıştır. Tam otomatik ve internete bağlı laboratuvarlar, coğrafi sınırların ötesinde veri sömürüsü ve biyolojik materyallerin manipülasyonu için fırsatlar sunmaktadır (United Kingdom Government, 2019). Bu laboratuvarlar, düzenlemelerin daha gevşek olduğu bölgelerde deneyler yapmak için kullanılabileceği gibi, bilgi güvenliği açıkları nedeniyle de risk taşımaktadır. Sentetik biyoloji ile gerçekleşebilecek suç örneklerine ilişkin öngörülen riskler arasında siber-biyosuç, biyolojik kötü amaçlı yazılımlar ve gen düzenlemesi bulunmaktadır. Siber-biyosuç, dijital ve biyolojik sistemlerin kesişiminden kaynaklanan yeni bir suç türüdür ve internete bağlı laboratuvarların güvenlik zafiyetlerinden yararlanmayı içermektedir (Elgabry vd., 2020; Murch vd., 2018; Richardson vd., 2019;). Biyolojik kötü amaçlı yazılımlar ise, bilgisayara uzaktan erişim sağlayarak biyolojik materyalleri manipüle etme potansiyeline sahiptir. Gen düzenleme teknolojilerinin gelişmesiyle birlikte, kötü niyetli aktörler tarafından yasa dışı ilaç üretimi ve evde gen düzenleme gibi suçlarda artma potansiyeline sahiptir. Özellikle tasarım bebekler gibi onaylanmamış ve düzenlenmemiş genetik iyileştirmeler, etik ve güvenlik açısından ciddi riskler taşımaktadır (Richardson vd., 2019; Prangono & Arabo, 2021).

Bu çalışma, sentetik biyoloji ve siber suçlar arasındaki önemli bağlantıları ortaya koymayı ve gelecekteki suçların tanınmasını ve önlenmesini sağlamayı hedeflemektedir. Ayrıca, bu alandaki güvenlik önlemlerinin, ulusal düzeyde politikalar ve iş birlikleriyle etkin bir şekilde şekillendirilmesi gerektiğini vurgulamaktadır. Çünkü siber-biyosuçlar, uluslararası çapta ciddi sonuçlar doğurabilecek ve toplumları derinden etkileyebilecek potansiyele sahiptir. Sonuç olarak, makale, bu önemli konuya dikkat çekmeyi, politika yapıcıları, uzmanları ve araştırmacıları bu alanda daha fazla çalışmaya teşvik etmeyi amaçlamaktadır. Bu inceleme, sentetik biyoloji ile ilişkili olan ve gelecekte meydana gelebilecek potansiyel suç örneklerini belirlemeyi ve bunları önlemek için alınabilecek önlemleri tartışmayı amaçlamaktadır. Siber güvenlik, biyoteknolojinin kötüye kullanımına karşı büyüyen tehdidi ele almakta ve siber ile biyoloji arasında ortaya çıkan riskleri yönetmek için politikaların geliştirilmesini savunmaktadır (CellPress, 2016).

1.1 Sentetik Biyoloji ve Kavramsal Tanımı

Sentetik biyoloji, organizmaların genetik materyallerinin tasarımı ve değiştirilmesi yoluyla yeni işlevler kazandırılmasını hedefleyen multidisipliner bir alandır. Bu disiplin, genetik mühendislik, moleküler biyoloji, bilgisayar bilimi ve biyoinformatik gibi çeşitli bilim alanlarını içermektedir. Sentetik biyoloji, biyolojik sistemleri anlama ve manipüle etme potansiyeli sayesinde birçok sektörde çeşitli uygulamalar sunmaktadır (Mueller, 2021; Murch vd., 2018; Richardson vd., 2019).

1.2 Sentetik Biyolojinin Yaygınlaşması ve Etkileri

Son yıllarda sentetik biyoloji, teknolojideki hızlı ilerlemeler ve maliyetlerin düşmesiyle giderek daha yaygın hale gelmiştir. İnsan genomunun dizilenmesinin maliyetinin azalması, bir zamanlar sadece uzman kurumlar tarafından yapılan çalışmaların artık daha erişilebilir hale gelmesini sağlamıştır. Bu durum, sentetik biyolojinin daha geniş bir kullanıcı kitlesi tarafından benimsenmesine ve popülerleşmesine yol açmıştır. Sentetik biyolojinin yaygınlaşması, birçok alanda önemli etkiler yaratmıştır. Tıp alanında, hastalıkların teşhis ve tedavisinde kullanılan genetik testler ve terapiler geliştirilmesi mümkün olmuştur. Tarım ve gıda sektöründe ise, bitkilerin genetik yapıları değiştirilerek daha verimli ve dayanıklı ürünler elde edilebilir hale

gelmiştir. Aynı zamanda, biyoteknoloji sayesinde endüstriyel süreçler daha çevre dostu ve verimli hale getirilmiştir (Elgabry, 2020; Richardson vd., 2019).

1.3 Siber Suçlar ve Sentetik Biyoloji Arasındaki İlişki

Sentetik biyolojinin ilerlemesi, aynı zamanda siber suçlarla ilişkilendirilebilecek yeni riskleri de beraberinde getirmiştir. Siber suçlar, bilgisayar sistemlerini hedef alarak veri sızdırma, manipülasyon ve çalma gibi faaliyetleri içeren suçlar olarak tanımlanmaktadır. Sentetik biyolojinin internete bağlı laboratuvarlar aracılığıyla kullanılabilir hale gelmesi, siber suçların biyolojik materyalleri manipüle etme ve biyolojik kötü amaçlı yazılımların kullanılmasıyla ilişkilendirilebileceği anlamına gelmektedir (Cummings vd., 2021; Peccoud, 2016; Trump vd., 2021). Özellikle, tam otomatik ve internete bağlı laboratuvarlar, siber saldırılar için yeni bir hedef oluşturabilir. Bu laboratuvarlar, düzenlemelerin daha gevşek olduğu bölgelerde faaliyet gösterebilir ve bilgi güvenliği açıklarından yararlanılabilir. Ayrıca, biyolojik kötü amaçlı yazılımlar, biyolojik materyalleri manipüle etmek ve organizmaların işlevlerini değiştirmek amacıyla kullanılabilir (Hamilton vd., 2021; Malsch, & Espona, 2021; Novossiolova, 2021).

2. SENTETİK BİYOLOJİ VE POTANSİYEL SUÇ FIRSATLARI

2.1 Biyolojik Ayrımcılık ve Mahremiyet Riskleri

Sentetik biyolojiden elde edilen büyük miktardaki biyolojik veriler, potansiyel olarak mahremiyet ve güvenlik risklerini beraberinde getirmektedir. Biyolojik verilerin toplanması, depolanması ve analiz edilmesi, kişisel ve sağlıkla ilgili hassas bilgiler içerir. Bu verilerin kötüye kullanımı, bireylerin özel bilgilerinin ifşa edilmesine, ayrımcılığa ve kişisel mahremiyetin ihlaline neden olabilir. Örneğin, sağlık sigortacıları, genomik verilere dayanarak kişilerin hastalık risklerini değerlendirebilir ve buna göre primlerini belirleyebilirler. Bu da biyolojik ayrımcılığa yol açabilir ve bireylerin sigorta koşullarını olumsuz yönde etkileyebilir (Elgabry, 2020; Richardson vd., 2019; Prangono, & Arabo, 2021).

2.2 Siber-Biyosuç ve İnternet Bağlantılı Laboratuvarlar

Günümüzde sentetik biyoloji laboratuvarları giderek daha fazla internet bağlantılı hale gelmektedir. Bu durum, laboratuvarlardaki ekipman ve süreçlerin dijital ağlar üzerinden uzaktan yönetilebilmesini sağlamaktadır. Ancak bu bağlantılar, siber suçların biyolojik materyaller üzerindeki kötü amaçlı etkilerini artırmaktadır. Siber-biyosuç, internet bağlantılı laboratuvarları hedef alarak biyolojik materyallerin manipülasyonunu ve çalınmasını içerebilir. Örneğin, düşman devletler, bilgisayar korsanları vasıtasıyla bir ülkedeki araştırma laboratuvarlarını hedef alarak değerli biyolojik verileri çalabilir ve başka yerlerde kullanabilirler (Novossiolova vd., 2021; Peccoud, 2016).

2.3 Biyolojik Kötü Amaçlı Yazılım ve Veri Hırsızlığı

Biyolojik kötü amaçlı yazılımlar, organizmaların genetik yapılarını değiştirme veya işlevlerini etkileme amacıyla tasarlanan zararlı yazılımlardır. Bu tür kötü amaçlı yazılımlar, gen düzenleme araçlarının internet bağlantılı laboratuvarlarda kullanılmasıyla potansiyel bir risk oluşturur. Bu yazılımlar, biyolojik materyallerin içine sızabilir ve organizmaların işlevlerini istenmeyen şekillerde değiştirerek ciddi biyolojik sonuçlara yol açabilir. Aynı zamanda, biyolojik veri hırsızlığı da büyük bir tehdittir. Biyolojik materyaller ve genetik veriler, değerli araştırmaların temelini oluşturur ve bu verilerin çalınması, bilimsel ilerlemenin engellenmesine ve ticari kazanç sağlamak isteyen kötü niyetli kişilerin eline geçmesine yol açabilir (Cummings vd., 2021; Peccoud, 2016; Trump vd., 2021).

2.4 Kötü Niyetli Biyolojik Korsanlık ve Gen Düzenleme

Gen düzenleme teknolojilerinin kolaylaşmasıyla, "biohacker" olarak adlandırılan bireylerin kendi başlarına genetik düzenlemeler yapma potansiyeli artmıştır. Bu, potansiyel olarak kötü niyetli bireylerin gen düzenleme araçlarını kullanarak yasa dışı faaliyetlere girişmesine olanak tanır. Kötü niyetli biyolojik korsanlık, belirli kişilere yönelik genetik düzenlemeler yaparak onları finansal olarak sömürmek veya zarar vermek amacıyla gerçekleştirilebilir. Aynı zamanda, tasarım bebekler gibi onaylanmamış ve düzenlenmemiş genetik iyileştirmeler sağlayan karaborsalar da ortaya çıkabilir. Bu tür kötü amaçlı gen düzenlemeleri, etik ve hukuki açıdan önemli sorunlar doğurabilir ve insan sağlığını ciddi şekilde tehlikeye atabilir (Cummings vd., 2021; Hamilton vd., 2021).

2.5 Evde Yasadışı Uyuşturucu Üretimi ve Karaborsalar

Sentetik biyolojinin yaygınlaşmasıyla, evde yasadışı uyuşturucu üretimi konusunda yeni fırsatlar ortaya çıkmıştır. Biohackerlar, gen düzenleme tekniklerini kullanarak yeni psikoaktif maddeler yaratabilir ve yasadışı ilaçlar üretebilir. Bu tür uyuşturucu üretimi, merkezi otoritelerin kontrolü dışında gerçekleştirilebilir ve uyuşturucu kaçakçılığını kolaylaştırabilir. Kötü niyetli bireyler, karaborsalarda yasadışı ilaç satışı yapabilir ve bu tür faaliyetlerden yararlanarak ticari kazanç elde edebilirler. Bu durum, sağlık ve güvenlik risklerini artırabilir ve toplumda tehlikeli sonuçlar doğurabilir (Malsch & Espona, 2021; Novossiolova vd., 2021).

3. SENTETİK BİYOLOJİDE SUÇ ÖNLEME VE TESPİT STRATEJİLERİ

Sentetik biyolojinin potansiyel suç fırsatlarına yönelik önleme ve tespit stratejileri, multidisipliner bir yaklaşım gerektirir. Hem bilim insanları hem de güvenlik uzmanları, sentetik biyolojinin gelişimini takip ederek potansiyel suçların tanınmasında iş birliği yapmalıdır. Bu bölümde, sentetik biyolojide suç önleme ve tespitine yönelik bazı stratejiler ele alınmaktadır (Adler vd., 2021; Cummings vd., 2021; Malsch & Espona, 2021).

3.1 Biyoteknoloji ve Siber Güvenlik Uzmanlarının İş Birliği

Sentetik biyolojiyle ilgili suç önleme ve tespit stratejileri, bilim insanları ve siber güvenlik uzmanları arasındaki iş birliğini içermelidir. Biyoteknoloji uzmanları, sentetik biyoloji alanındaki gelişmeleri takip ederek potansiyel suç fırsatlarını belirlemeye yardımcı olabilirler. Aynı zamanda, siber güvenlik uzmanları da internet bağlantılı laboratuvarlardaki güvenlik açıklarını tespit ederek siber saldırılara karşı önlemler alabilirler. Bilim insanları ile güvenlik uzmanlarının birlikte çalışması, sentetik biyolojideki suç potansiyelini azaltmaya yardımcı olabilir (Appleton, & Millett, 2021; Jin, & Linkov, 2021; Nieuwenweg vd.,2021).

3.2 Biyolojik Malzemelerin İzlenmesi ve Güvenliği

Biyolojik malzemelerin izlenmesi ve güvenliği, potansiyel suçların önlenmesinde kritik bir rol oynamaktadır. Biyolojik malzemelerin hareketini ve kullanımını izlemek, kötü niyetli faaliyetleri tespit etmede yardımcı olabilir. Biyolojik malzemelerin laboratuvar dışına çıkışı ve girişi sıkı bir şekilde kontrol edilmelidir. Ayrıca, laboratuvarlarda biyolojik materyallerin güvenli bir şekilde saklandığından ve yetkisiz erişime karşı korunduğundan emin olunmalıdır (Barbato, 2021; Nelson vd., 2021; Rhodes & Lentzos, 2021).

3.3 Genetik Verilerin Güvenliği ve Mahremiyetin Korunması

Sentetik biyolojiyle ilgili önemli bir konu, genetik verilerin güvenliği ve mahremiyetidir. Genetik verilerin çalınması veya kötüye kullanılması, bireylerin özel bilgilerinin ifşa edilmesine ve biyolojik ayrımcılığa neden olabilir. Bu nedenle, genetik verilerin güvenli bir şekilde saklandığından ve yetkisiz kişilerin erişimine karşı korunduğundan emin olunmalıdır. Ayrıca, genetik verilerin kullanımıyla ilgili etik kuralların ve yasal düzenlemelerin uygulanması da önemlidir (Florin & Trump, 2021.; Murch & Linkov, 2021).

3.4 Eğitim ve Farkındalık Oluşturma

Sentetik biyolojideki suç potansiyelini azaltmanın bir yolu da eğitim ve farkındalık oluşturmaktır. Hem bilim insanları hem de genel halk, sentetik biyolojinin potansiyel suçlara yönelik risklerini anlamalı ve bu konuda bilinçlenmelidir. Bilim insanları, güvenlik uzmanları ve diğer paydaşlar, sentetik biyolojiyle ilgili suç önleme ve tespit stratejilerini halka açıklamalı ve eğitim programları düzenlemelidir. Bu sayede, potansiyel suçlarla mücadelede daha etkili bir toplumsal bilinç oluşabilir (Murch vd., 2018; Nelson vd., 2021).

3.5 Ulusal ve Uluslararası İş Birliği

Sentetik biyolojideki suç potansiyelini önlemek ve tespit etmek için ulusal ve uluslararası düzeyde iş birliği önemlidir. Ülkeler, sentetik biyolojiyle ilgili suçlarla mücadelede birlikte çalışmalı ve bilgi paylaşımını teşvik etmelidir. Uluslararası düzeyde siber-biyogüvenlik politikaları ve standartlar oluşturmak, potansiyel suçların önlenmesinde ve uluslararası suçluların tespit edilmesinde etkili olabilir. Aynı zamanda, uluslararası iş birliği, yeni suç fırsatlarının ortaya çıktığı coğrafi ve kültürel çeşitlilik dikkate alınarak daha kapsamlı ve etkili bir suç önleme stratejisi oluşturulmasına katkı sağlayabilir (Appleton & Millett, 2021; Barbato, 2021). Bu stratejiler, sentetik biyolojiyle ilgili suçları önlemeye ve tespit etmeye yönelik olarak multidisipliner bir yaklaşımın benimsenmesini vurgulamaktadır. Biyoteknoloji uzmanları, siber güvenlik uzmanları, bilim insanları ve diğer paydaşlar, sentetik biyolojinin etik ve güvenli bir şekilde kullanılmasını sağlamak için birlikte çalışmalı ve toplumsal fayda odaklı bir yaklaşım benimsemelidirler. Ancak sürekli gelişen teknolojik ortamda suç önleme

ve tespit stratejilerinin sürekli olarak güncellenmesi ve iyileştirilmesi de önemlidir. Bu sayede, gelecekteki suçların tanınması ve önlenmesi için proaktif bir yaklaşım benimsenmiş olur (Murch vd., 2018; Nelson vd., 2021).

4. SENTETİK BİYOLOJİ VE GELECEKTEKİ SUÇLARIN TANINMASI

Sentetik biyoloji alanındaki hızlı gelişmeler ve teknolojinin yaygınlaşması, gelecekte yeni suç fırsatlarının ortaya çıkmasına neden olacaktır. Bu bölümde, sentetik biyolojinin gelecekteki suçlar açısından potansiyel riskleri ve tanınması gereken önemli konular ele alınacaktır.

4.1 Biyoteknolojinin Hızlı Gelişimi ve Suç Potansiyeli

Sentetik biyoloji alanındaki hızlı teknolojik gelişmeler, yeni suç fırsatlarının ortaya çıkmasına neden olacaktır. Özellikle DNA sentezi teknolojisinin gelişmesi ve maliyetinin düşmesi, biyolojik malzemelerin kolaylıkla elde edilmesini ve manipüle edilmesini sağlamaktadır. Bu durum, genetik mühendislik ve biyolojik düzenlemelerin kötü niyetli amaçlarla kullanılma olasılığını artırmaktadır (Lewis & Linkov, 2020; Peccoud vd., 2018; Richardson vd., 2019).

4.2 Genetik Şantaj ve Manipülasyon Tehlikesi

Gelecekte, genetik verilerin daha yaygın bir şekilde toplanması ve saklanması beklenmektedir. Bu durum, genetik verilerin kötü niyetli kişilerin eline geçme riskini artırabilir. Genetik şantaj, bir bireyin DNA bilgilerinin gasp edilerek onunla ilgili tehdit veya manipülasyon yapılması durumunu ifade eder. Özellikle kişisel bilgilerin çalınması ve genetik verilerin internet üzerinden kötüye kullanılması, insanları potansiyel risklere karşı savunmasız hale getirebilir (George, 2019; Millett vd., 2019).

4.3 Artan İnternet Bağlantılı Laboratuvarların Güvenliği

İleriki yıllarda internet bağlantılı laboratuvarların sayısında artış beklenmektedir. Bu laboratuvarlar, uzaktan erişim ve otomasyon sayesinde coğrafi sınırları aşan deneylerin yapılmasına imkan tanırken, aynı zamanda siber saldırılara karşı da açık hale gelebilirler. Siber-biyosuç, internet bağlantılı laboratuvarların güvenliğine yönelik risklerin arttığı bir alandır. Bu tür laboratuvarların güvenliğinin sağlanması, potansiyel suçların önlenmesinde kritik bir rol oynayacaktır (Appleton & Millett, 2021; Murch & Linkov, 2021; Rhodes & Lentzos, 2021).

4.4 Biyolojik Terör Tehdidi

Biyolojik terör tehdidi, günümüzde teknolojik gelişmelerin hızlanması ve biyoteknoloji alanında yapılan ilerlemelerle artan bir endişe kaynağıdır. Sentetik biyoloji, genetik mühendislik ve biyolojik düzenlemeler gibi alanlardaki ilerlemeler, insanlara zarar verme potansiyeline sahip patojenlerin ve mikroorganizmaların oluşturulması veya modifiye edilmesiyle sonuçlanabilir. Bu tür kötü niyetli eylemler biyolojik terör saldırıları olarak adlandırılır.

Biyolojik terör saldırıları, biyolojik ajanların (virüsler, bakteriler, zehirli maddeler vb.) kullanılmasıyla gerçekleştirilen ve insan sağlığına ve toplum düzenine ciddi zararlar verebilecek eylemlerdir. Bir biyolojik terör saldırısının sonuçları, özellikle doğru tedbirler alınmadığı takdirde, oldukça yıkıcı ve yayılabilir nitelikte olabilir (CellPress, 2016; Trump, 2021;).

Sentetik biyoloji ve genetik mühendislik, bilimsel ve tıbbi ilerlemeler için oldukça faydalı olmakla birlikte, yanlış ellerde kullanıldığında ciddi tehditler oluşturabilir. Örneğin, mevcut patojenlerin genetik yapıları üzerinde değişiklikler yaparak daha virülan ve dirençli hale getirilebilirler. Böylece, mevcut aşıların veya ilaçların etkisiz kalmasına ve hastalıkların yayılmasına yol açabilirler. Bu nedenle, biyoteknoloji alanındaki gelişmelerin yakından takip edilmesi ve bu teknolojilerin güvenli kullanımını sağlamak için düzenlemelerin sıkılaştırılması gereklidir. Araştırmacılar ve bilim insanları, etik kurallara uygun şekilde çalışmalarını sürdürerek potansiyel kötüye kullanımları önlemeye katkı sağlamalıdırlar.

Biyolojik terör tehdidine karşı alınacak önlemler, erken uyarı sistemlerinin ve izleme mekanizmalarının geliştirilmesiyle başlar. Potansiyel saldırıları önceden tespit ederek önlem almak, büyük salgınların ve acil durumların önüne geçebilir. Ayrıca, biyolojik ajanların depolanması ve kullanımı konusunda sıkı kontroller uygulanması, bu tür tehditlerin oluşmasını engellemeye yardımcı olabilir (Elgabry, 2020; Peccoud, 2016).

Halkın ve sağlık çalışanlarının bilinçlendirilmesi de biyolojik terör saldırılarına karşı alınacak önlemlerde

önemli bir rol oynar. Acil durum planları hazırlamak, hızlı ve etkili tepki verme yeteneğini arttırabilir. Bu gibi hazırlıklar, saldırı sonrası etkilerin en aza indirilmesine ve toplumun güvenliğinin sağlanmasına yardımcı olabilir. Son olarak, uluslararası iş birliği ve bilgi paylaşımı da biyolojik terör tehdidiyle mücadelede önemli bir faktördür. Bu tür saldırıların sınır tanımaz nitelikte olması nedeniyle ülkeler arasındaki iş birliği ve koordinasyon, daha etkili ve kapsamlı önlemlerin alınmasına yardımcı olabilir.

Biyolojik terör tehdidi, bilgi ve teknolojideki hızlı ilerlemelerle birlikte devam edecek bir risktir. Ancak bilinçli ve koordineli bir şekilde önlemler alındığında, bu tür tehditlerin etkisi minimize edilebilir ve toplumların güvenliği korunabilir (Adler vd., 2021; Jin & Linkov, 2021).

4.5 Sosyal ve Etik Sorunlar

Sentetik biyolojinin gelişimi, sosyal ve etik sorunları da beraberinde getirecektir. Özellikle genetik mühendislik ve gen düzenleme gibi teknolojilerin etik sınırlarının belirlenmesi zor olabilir. Tasarım bebekler, genetik iyileştirmeler ve biyolojik kötü amaçlı yazılım gibi konular, toplumda etik tartışmaları tetikleyebilir ve potansiyel suçların kökenini oluşturabilir. Bu tür sosyal ve etik sorunların belirlenmesi ve ele alınması, gelecekteki suçların önlenmesinde önemli bir adım olacaktır (Nieuwenweg vd., 2021).

Sentetik biyoloji alanındaki gelişmeler, potansiyel suçların tanınması ve önlenmesi için sürekli bir dikkat ve özen gerektirmektedir. Bilim insanları, güvenlik uzmanları ve toplumun diğer paydaşları, bu alandaki gelişmeleri yakından takip ederek, yeni suç fırsatlarına karşı etkili önlemler almalı ve toplumu bilinçlendirmelidir. Aynı zamanda, ulusal ve uluslararası iş birliğiyle sentetik biyolojinin güvenli ve etik kullanımı sağlanabilir ve gelecekteki suçların önüne geçilebilir (Appleton & Millett, 2021; Barbato,2021; Rhodes & Lentzos 2021).

5. SUÇ ÖNLEME VE MÜCADELE STRATEJİLERİ

Gelecekteki suçların önlenmesi ve mücadele edilmesi için etkili stratejiler geliştirmek, sentetik biyoloji ve siber-biyosuç alanlarında önemli bir zorluktur. Bu bölümde, suç önleme ve mücadele için önerilen bazı stratejiler ele alınacaktır.

5.1 Yasal Düzenlemeler ve Denetimler

Sentetik biyolojinin hızla gelişmesi, mevcut yasal düzenlemelerin bu alana yetişmesini zorlaştırmıştır. Bu nedenle, gelecekteki suçların önlenmesi ve toplumun güvenliğinin sağlanması için, ulusal ve uluslararası düzeyde uygun yasal düzenlemeler ve denetimler yapılması gerekmektedir. Yasal düzenlemelerin sentetik biyoloji ve siber-biyosuç alanlarını kapsayan bir çerçeve sunması önemlidir. Genetik mühendislik ve biyolojik düzenlemeler gibi teknolojilerin etik sınırlarını belirlemek, potansiyel suçların önlenmesinde kritik bir rol oynar. Yasal düzenlemeler, bu teknolojilerin kötü niyetli kullanımını önlemek için etkili önlemler içermelidir. Ulusal ve uluslararası düzeyde uyumlu yasal düzenlemelerin oluşturulması için iş birliği önemlidir. Ülkeler arası iş birliği ve bilgi paylaşımı, sentetik biyoloji ve siber-biyosuç alanlarında karşılaşılan potansiyel risklerin daha iyi anlaşılmasına ve etkili denetim mekanizmalarının oluşturulmasına katkı sağlar (Florin & Trump, 2021.; Murch & Linkov, 2021). Uluslararası düzeyde oluşturulacak standartlar ve kılavuzlar, ülkelerin kendi yasal düzenlemelerini belirlerken bir temel oluşturabilir. Bununla birlikte, yasal düzenlemelerin sadece teknolojik unsurlarla sınırlı kalmaması önemlidir. Özellikle sentetik biyoloji gibi yeni ve potansiyel riskler taşıyan alanlarda, etik değerler ve toplumsal kabul önemlidir. Yasal düzenlemeler, etik komiteler ve toplumsal paydaşlarla birlikte oluşturulmalı ve gelecekteki suçları önlemeye yönelik stratejiler içermelidir (Barbato, 2021; Peccoud vd., 2018). Aynı zamanda, internet bağlantılı laboratuvarların güvenliğini sağlamak için de etkili yasal düzenlemeler yapılmalıdır. Bu laboratuvarlarda kullanılan yazılımların güvenliği ve siber saldırılara karşı korunması önemlidir. Yasal düzenlemeler, laboratuvarların güvenliğini artırmak için uygun denetim mekanizmaları ve güvenlik standartları içermelidir. Sonuç olarak;, sentetik biyoloji ve siber-biyosuç alanlarında gelecekteki suçların önlenmesi ve toplumun güvenliğinin sağlanması için uygun yasal düzenlemeler ve denetimler büyük önem taşır. Yasal düzenlemelerin etik sınırların belirlenmesi, kötü niyetli kullanıma karşı önlemler alınması ve laboratuvarların güvenliğinin sağlanması gibi konuları kapsaması, bu alanda etkin bir mücadele için gereklidir. Ulusal ve uluslararası iş birliği ve toplumsal paydaşlarla birlikte yürütülen çalışmalar, sentetik biyoloji alanındaki potansiyel risklerin önlenmesine ve toplumun güvenliğinin sağlanmasına önemli katkılar yapacaktır (Millett vd., 2019).

5.2 Ulusal ve Uluslararası İş Birliği

Suç önleme ve mücadelede etkili bir şekilde çalışabilmek için ulusal ve uluslararası düzeyde iş birliği önemlidir. Farklı ülkeler, akademisyenler, bilim insanları ve güvenlik uzmanları arasında bilgi ve istihbarat paylaşımı, gelecekteki suçların tanınması ve önlenmesi açısından kritik bir rol oynar. Uluslararası iş birliği, sentetik biyoloji ve siber-biyosuç alanlarında karşılaşılan potansiyel risklerin daha iyi anlaşılmasına ve etkili denetim mekanizmalarının oluşturulmasına katkı sağlar. Uluslararası düzeyde iş birliği, ortak stratejilerin geliştirilmesine ve uygulanmasına olanak tanır. Farklı ülkelerdeki sentetik biyoloji araştırmaları ve laboratuvarlarında yaşanan deneyimlerin paylaşılması, bu alanda karşılaşılan potansiyel suçların daha iyi anlaşılmasına yardımcı olur. Bu iş birliği sayesinde, ortak riskler belirlenir ve bunlara karşı etkili önlemler alınabilir. Bilgi ve istihbarat paylaşımı, sentetik biyoloji ve siber-biyosuç alanlarında karşılaşılan tehditlerin zamanında tespit edilmesine yardımcı olur. Böylece, potansiyel suçların tanınması ve önlenmesi için daha hızlı ve etkili adımlar atılabilir. Uluslararası iş birliği sayesinde, farklı ülkelerdeki güvenlik uzmanları ve yetkililer, sentetik biyoloji alanında gerçekleşen gelişmeleri ve potansiyel riskleri izleyebilir, ortak bir anlayış oluşturabilir ve güvenlik politikalarını buna göre şekillendirebilir (Florin & Trump, 2021; Murch & Linkov, 2021). Uluslararası anlaşmalar ve iş birliği mekanizmalarının geliştirilmesi, sentetik biyoloji ve siber-biyosuç alanlarında etkili bir suç önleme ve mücadele stratejisi oluşturulmasına yardımcı olur. Bu anlaşmalar, farklı ülkeler arasında ortak hedeflerin belirlenmesine ve bu hedeflere ulaşmak için koordineli çalışmalara imkân tanır. Böylece, sentetik biyoloji alanında gerçekleşen gelişmelerin toplumlar için güvenli ve sorumlu bir şekilde kullanılması sağlanabilir. Sonuç olarak, ulusal ve uluslararası düzeyde iş birliği, sentetik biyoloji ve siber-biyosuç alanlarında gelecekteki suçların önlenmesi ve toplumun güvenliğinin sağlanması için kritik öneme sahiptir. Bilgi ve istihbarat paylaşımı, ortak stratejilerin geliştirilmesi ve uluslararası anlaşmalar sayesinde, sentetik biyoloji alanındaki potansiyel riskler daha etkili bir şekilde izlenerek, toplumun güvenliği ve refahı korunabilir. Bu nedenle, tüm paydaşların ulusal ve uluslararası düzeyde iş birliği içinde çalışması ve sentetik biyoloji alanında etkili suç önleme ve mücadele stratejilerinin geliştirilmesi önemlidir (George, 2019; Lewis & Linkov, 2020; Richardson vd., 2019).

5.3 Eğitim ve Farkındalık Oluşturma

Toplumun genelinde sentetik biyoloji ve siber-biyosuç konularına ilişkin farkındalık düzeyinin arttırılması önemlidir. Bu konuda eğitim kurumları, kamu kurumları ve medyanın rolü büyük öneme sahiptir. Eğitim kurumları, sentetik biyoloji ve siber-biyosuç hakkında bilinçlendirme programları düzenleyerek, öğrencilerin ve genç araştırmacıların bu alanlardaki etik ve güvenlik konularını anlamalarına yardımcı olabilir (Jin & Linkov, 2021; Nieuwenweg vd., 2021). Aynı zamanda, halka yönelik bilgilendirme etkinlikleri ve seminerler düzenlemek, geniş kitlelerin bu konularda bilinçlenmesini sağlayabilir. Kamu kurumları da toplumda farkındalık oluşturmak için önemli bir rol oynar. Kamu kurumları, sentetik biyoloji ve siber-biyosuç hakkında bilgilendirici materyaller hazırlayarak, vatandaşların potansiyel riskler konusunda bilinçlenmelerini sağlayabilir. Ayrıca, halka açık etkinlikler ve kampanyalar düzenlemek, toplumun bu konulardaki farkındalık düzeyini arttırmak için etkili bir yöntem olabilir (Florin & Trump, 2021; Murch vd., 2018). Medya da bu konuda etkili bir araçtır. Haberler, makaleler ve televizyon programları aracılığıyla, sentetik biyoloji ve siber-biyosuç konularına ilişkin güvenilir bilgi ve haberlerin yayınlanması, halkın bu alanlardaki gelişmeler hakkında bilgi sahibi olmasına katkı sağlar. Medyanın doğru ve tarafsız bilgi verme sorumluluğu, toplumun bilinçlenmesi ve potansiyel risklerin fark edilmesi açısından kritik bir rol oynar. Bunun yanı sıra, bilim insanları ve güvenlik uzmanları arasında multidisipliner eğitim ve iş birliğinin teşvik edilmesi de önemlidir. Sentetik biyoloji ve siber-biyosuç alanlarında çalışan uzmanlar, farklı disiplinlerden gelen bilim insanlarıyla biraraya gelerek, bu konulardaki gelişmeleri daha etkili bir şekilde izleyebilir ve değerlendirebilirler (Murch & Linkov, 2021). Birlikte çalışarak, potansiyel risklerin belirlenmesi ve gelecekteki suçların önlenmesi için daha güçlü bir ekip oluşturulabilir. Sonuç olarak, sentetik biyoloji ve siber-biyosuç alanlarında potansiyel suçların önlenmesi ve toplumun güvenliğinin sağlanması için eğitim ve farkındalık oluşturma çabaları büyük önem taşır. Eğitim kurumları, kamu kurumları, medya ve uzmanlar arasındaki iş birliği, toplumun bu konulardaki bilgi düzeyini arttırabilir ve potansiyel riskleri önceden fark etmeye yardımcı olabilir. Tüm paydaşların aktif katılımı ve iş birliği, sentetik biyoloji ve siber-biyosuç alanlarında güvenli ve etik bir ortamın oluşturulmasına ve toplumun gelecekteki suçlara karşı daha güvenli olmasına katkı sağlayacaktır (Lewis & Linkov, 2020).

5.4 Etik Komiteler ve İzleme Mekanizmaları

Sentetik biyoloji alanında çalışan araştırmacılar ve bilim insanları, etik komiteler ve izleme mekanizmaları ile iş birliği yapmalıdır. Etik komiteler, araştırma ve geliştirme süreçlerinde etik standartların korunmasına ve kötü niyetli kullanıma karşı önlemlerin alınmasına yardımcı olabilir. Bu komiteler, sentetik biyoloji teknolojisinin etik kurallara uygun bir şekilde kullanılmasını teşvik ederek, potansiyel riskleri önceden tanımaya ve önlemeye yardımcı olur. Araştırmaların etik açıdan değerlendirilmesi, bilimsel toplumun güvenini sağlamak ve toplumun refahını korumak açısından önemlidir. Ayrıca, sentetik biyoloji alanındaki araştırmaları izlemek ve potansiyel suçları tanımak için etkili izleme mekanizmalarının oluşturulması önemlidir. Bu mekanizmalar, araştırma laboratuvarlarında ve endüstriyel tesislerde kullanılacak sentetik biyoloji teknolojilerinin kullanımını takip edebilir ve izleyebilir. Bu sayede, yasadışı veya kötü niyetli kullanıma ilişkin şüpheli aktiviteler tespit edilebilir ve önlem alınabilir. Aynı zamanda, izleme mekanizmaları, potansiyel risklerin belirlenmesine ve gelecekteki suçların önlenmesine yardımcı olabilir (Novossiolova vd., 2021). Etik komiteler ve izleme mekanizmaları arasında sıkı bir iş birliği, sentetik biyoloji alanındaki etik ve güvenlik standartlarının sürekli olarak güncellenmesine yardımcı olabilir. Bu iki mekanizma, yeni tehditlere karşı duyarlılık geliştirmek ve teknolojik gelişmeleri yakından takip etmek için düzenli olarak bir araya gelmeli ve bilgi paylaşımında bulunmalıdır. Ayrıca, uluslararası iş birliği, farklı ülkelerdeki etik kuralların ve izleme mekanizmalarının uyumlaştırılmasına yardımcı olabilir ve sentetik biyoloji alanında küresel bir etik çerçeve oluşturabilir (Jin & Linkov, 2021). Sonuç olarak, sentetik biyoloji alanında potansiyel suçların önlenmesi ve toplumun güvenliğinin sağlanması için etik komitelerin ve izleme mekanizmalarının etkin bir şekilde kullanılması büyük önem taşır. Etik standartların korunması, potansiyel risklerin belirlenmesi ve teknolojik güvenlik önlemlerinin alınması, sentetik biyoloji teknolojisinin sorumlu ve etik bir şekilde kullanılmasına katkı sağlayacaktır. Tüm paydaşların iş birliği içinde çalışması ve etik kurallara uygun bir şekilde davranması, sentetik biyoloji alanının olumlu etkilerinin arttırılmasına ve potansiyel risklerin minimize edilmesine yardımcı olacaktır (Elgabry, 2020; Hamilton vd., 2021; Prangono & Arabo, 2021).

5.5 Teknolojik Güvenlik ve Veri Koruma

Gelecekteki suçların önlenmesi için teknolojik güvenlik ve veri koruma önlemleri almak kritik öneme sahiptir. Özellikle internet bağlantılı laboratuvarlar ve biyoteknoloji sistemlerinin güvenliği sağlanmalıdır. Kötü niyetli yazılımların ve siber saldırıların önüne geçmek için etkili güvenlik önlemleri alınmalı ve verilerin korunması sağlanmalıdır. Teknolojik güvenlik önlemleri, sentetik biyoloji alanındaki laboratuvarlarda kullanılan yazılım ve donanımların güvenliğini sağlamayı içerir. Bu önlemler, laboratuvarlara yetkisiz erişimi önlemek, bilgisayar ağlarını korumak ve siber saldırılara karşı dayanıklılığı artırmak için alınabilir. Laboratuvarlardaki bilgisayar sistemlerinin güvenlik duvarlarıyla korunması ve giriş-çıkışların sıkı bir şekilde izlenmesi, kötü niyetli kişilerin laboratuvar içindeki verilere erişimini engelleyebilir. Ayrıca, biyoteknoloji sistemlerinin güvenliği de büyük önem taşır. Bu sistemlerin internete bağlı olması, kötü niyetli kişilerin uzaktan erişim sağlaması ve siber saldırılara maruz kalması potansiyel riskler arasındadır. Bu nedenle, biyoteknoloji şirketleri ve araştırma laboratuvarları, bu sistemlerin güvenliğini sağlamak için güçlü şifreleme teknolojileri, kimlik doğrulama protokolleri ve güvenli veri depolama yöntemleri kullanmalıdır. Veri koruma önlemleri de sentetik biyoloji alanında önemli bir role sahiptir. Araştırma verilerinin ve bilgilerinin korunması, bilimsel bilginin ve ticari sırların güvenliğini sağlamak açısından kritik öneme sahiptir. Veri depolama ve aktarım süreçlerinde güvenlik protokolleri kullanılmalı ve bilgilerin yetkisiz kişilerin eline geçmesini önlemek için gerekli tedbirler alınmalıdır. Bunun yanı sıra, sentetik biyoloji alanındaki güvenlik ve veri koruma önlemlerinin sürekli olarak güncellenmesi ve geliştirilmesi gerekmektedir. Teknolojideki hızlı değişim ve siber saldırı yöntemlerindeki sürekli ilerleme, güvenlik önlemlerinin etkinliğini sürdürmek için sürekli bir çaba gerektirir. Bu nedenle, güvenlik uzmanları, araştırmacılar ve endüstri temsilcileri arasında iş birliği ve bilgi paylaşımı teşvik edilmelidir. Tüm bu teknolojik güvenlik ve veri koruma önlemlerinin bir araya gelerek uygulanması, sentetik biyoloji alanındaki potansiyel suçların önlenmesine ve toplumun güvenliğinin sağlanmasına yardımcı olacaktır. Böylece, bu hızla gelişen alanda gelecekte ortaya çıkabilecek suçlara karşı güçlü bir savunma mekanizması oluşturulabilir ve sentetik biyoloji teknolojisinin pozitif etkileri, toplumun refahı için en iyi şekilde kullanılabilir (Florin & Trump, 2021; Peccoud vd., 2018; Richardson vd., 2019).

6. SONUÇ

Sentetik biyolojinin ilerlemesi, yeni suç türlerinin ortaya çıkmasının yanı sıra, kötü niyetli kişilerin fırsatları değerlendirmesini de beraberinde getirmektedir. Bu nedenle, sentetik biyoloji alanında faaliyet gösteren tüm paydaşların suç önleme ve mücadele stratejilerine odaklanması kritik öneme sahiptir. Öncelikli olarak, ulusal ve uluslararası düzeyde yasal düzenlemelerin oluşturulması ve uygulanması gereklidir. Bu düzenlemeler, sentetik biyolojiyle ilişkili suçları tanımlamak ve etkin bir şekilde cezalandırmak için gerekli önlemleri içermelidir. Ayrıca, bu düzenlemeler, bilimsel araştırmaların etik ve güvenlik standartlarına uygun olarak yürütülmesini sağlamak için de önemli bir rol oynamaktadır. Teknolojik güvenlik önlemleri de sentetik biyolojiyle ilişkili suçların önlenmesinde kritik bir unsurdur. Biyogüvenlik ve veri koruma önlemleri, kötü niyetli kişilerin sentetik biyoloji teknolojilerini kötü amaçlarla kullanmasını engellemeye yardımcı olabilir. Aynı zamanda, bu önlemler, bilgi ve materyal akışlarını izlemeyi ve gerektiğinde müdahale etmeyi mümkün kılarak potansiyel suçları tespit etmeye yardımcı olabilir. Toplumda farkındalık oluşturma ve eğitim de suç önleme ve mücadele stratejilerinin etkili bir parçasıdır. Halkın sentetik biyoloji hakkında bilgilendirilmesi, potansiyel riskleri ve etik konuları anlamalarına yardımcı olabilir. Aynı zamanda, bilinçli ve bilgili bir toplum, kötü amaçlı faaliyetlere karşı daha duyarlı olabilir ve yetkililere şüpheli durumları bildirme konusunda daha istekli olabilir. Bunun yanı sıra, etik komitelerin kurulması ve izleme mekanizmalarının oluşturulması da önemlidir. Bu komiteler ve mekanizmalar, sentetik biyoloji uygulamalarının etik ve güvenlik standartlarına uygun olarak gerçekleştirilmesini sağlamak için denetim yapabilir ve gerekirse düzeltici önlemler alabilir. Son olarak, sentetik biyoloji alanındaki gelişmelerin dikkatle takip edilmesi ve öngörülemeyen risklerin önüne geçilmesi için sürekli bir bilgi paylaşımı ve iş birliği gereklidir. Bilim insanları, akademisyenler, endüstri temsilcileri ve hükümetler arasında etkili bir iletişim ağı kurulması, potansiyel suçların tanınması ve önlenmesine yardımcı olabilir. Tüm bu stratejilerin bir araya gelerek uygulanması, sentetik biyoloji alanındaki potansiyel suçların önlenmesinde ve toplumun güvenliğinin sağlanmasında önemli bir rol oynayacaktır. Böylece, sentetik biyoloji teknolojilerinin olumlu yönleri maksimum fayda sağlarken, potansiyel riskler en aza indirilebilir ve toplumun refahı korunabilir.

KAYNAKLAR

Adler, A., Beal, J., Lancaster, M., & Wyschogrod, D. (2021). Cyberbiosecurity and Public Health in the Age of COVID-19. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 103-115.

Appleton, E., & Millett, P. (2021). Technical Aspects of Biosecurity: Screening Guidance, Attribution, and Traceability. Emerging Threats of Synthetic Biology and Biotechnology. NATO Science for Peace and Security, 141-167.

Barbato, R. A. (2021). The Soil Habitat and Considerations for Synthetic Biology. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 169-175.

CellPress (2016). Synthetic biology used to limit bacterial growth and coordinate drug release.

Cummings, C. L., Volk, K. M., Ulanova, A. A., Lam, D. T. U. H., & Ng, P. R. (2021). Emerging Biosecurity Threats and Responses: A Review of Published and Gray Literature. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 13-36.

Elgabry, M., (2020). Written evidence submitted by Mariam Elgabry to the United Kingdom Biosecurity and National Security Joint Committee.Retrieved from https://committees.parliament.uk/writtenevidence/6854/pdf/

Elgabry, M., Nesbeth, D., & Johnson, S. D. (2020). A systematic review of the criminogenic potential of synthetic biology and routes to future crime prevention. Frontiers in bioengineering and biotechnology, 8, 1119.https://doi.org/10.3389/fbioe.2020.01119

Florin M.V., & Trump B.D.(2021). Conclusions on cyberbiosecurity governance.In B.D.Trump, et al.(Eds.), Emerging threats of synthetic biology and biotechnology: Addressing security and resilience issues (pp. 221-228). Springer Nature.

George, A. M. (2019). The national security implications of cyberbiosecurity. Frontiers in bioengineering and biotechnology, 7, 51.

Hamilton, R. A., Mampuys, R., Galaitsi, S. E., Collins, A., Istomin, I., Ahteensuu, M., & Bakanidze, L. (2021).

Opportunities, Challenges, and Future Considerations for Top-Down Governance for Biosecurity and Synthetic Biology. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 37-58.

Jin, A., & Linkov, I. (2021). Synthetic Biology Brings New Challenges to Managing Biosecurity and Biosafety. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 117-129.

Lewis, S.M., & Linkov I.(2020). Cyberbiosecurity: A call for cooperation in a new threat landscape.Frontiers in bioengineering and biotechnology, 8, 1119. https://doi.org/10.3389/fbioe.2020.01119

Malsch, I., & Espona, M. (2021). Responsible Governance of Biosecurity in Armenia. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 67-80.

Millett, K., Dos Santos, E., & Millett, P. D. (2019). Cyber-biosecurity risk perceptions in the biotech sector. Frontiers in bioengineering and biotechnology, 7, 136.

Mueller, S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?. Biosafety and health, 3(1), 11-21. https://doi.org/10.1186/s42522-021-00032-8

Murch R.S., & Linkov I.(2021). Cyberbiosecurity risk assessment framework.In B.D.Trump, et al.(Eds.), Emerging threats of synthetic biology and biotechnology: Addressing security and resilience issues (pp. 207-220). Springer Nature.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Frontiers in bioengineering and biotechnology, 39.https://doi.org/10.1016/j.tibtech.2017.10.012

Nelson, C., Adiguzel, I., Florin, M. V., Lentzos, F., Knutsson, R., Rhodes, C., ... & Vergin, A. (2021). Foresight in Synthetic Biology and Biotechnology Threats. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 177-194.

NHGRI. (N.d.). (2021). The cost of sequencing a human genome. Retrieved from https://www.genome.gov/about-genomics/fact-sheets/Sequencing-Human-Genome-cost. (Erişim 20.05.2024)

Nieuwenweg, A.C., et al. (2021). Emerging biotechnology and information hazards.In B.D.Trump, et al.(Eds.), Emerging threats of synthetic biology and biotechnology: Addressing security and resilience issues (pp. 131-140). Springer Nature.

Novossiolova, T., Kuiken, T., DeCoste, J., Henry, L., Malsch, I., Merad, M., ... & Waskow, A. (2021). Addressing emerging synthetic biology threats: the role of education and outreach in fostering effective bottom-up grassroots governance. Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 81-102.

Peccoud, J. (2016). Synthetic Biology: fostering the cyber-biological revolution. Synthetic Biology, 1(1), ysw001.. https://doi.org/10.1093/synbio/ysw001

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. Trends in biotechnology, 36(1), 4-7.https://doi.org/10.1016/j.tibtech.2017.10.012

Prangono, B. ve Arabo, A. (2021). COVID-19 pandemik siber güvenlik sorunları. İnternet Teknolojisi Mektupları, 4 (2), e247.https://doi.org/10.1002/itl2.247

Retrieved from https://www.sciencedaily.com/releases/2016/06/160630135852.htm

Rhodes, C., & Lentzos F.(2021). Governance challenges for emerging technologies with dual-use potential.In B.D.Trump, et al.(Eds.), Emerging threats of synthetic biology and biotechnology: Addressing security and resilience issues (pp. 193-206). Springer Nature.

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: a call for cooperation in a new threat landscape. Frontiers in bioengineering and biotechnology, 7, 451363.https://doi.org/10.3389/fbioe.2019.00099

Trump, B. D., Florin, M. V., Perkins, E., & Linkov, I. (2021). Emerging threats of synthetic biology and biotechnology: addressing security and resilience issues.. https://doi.org/10.1007/978-94-024-2086-9

United Kingdom Government (2019). Future technology trends in security. Retrieved from https://www.gov.uk/government/publications/future-technology-trends-in-security