

EDITORIAL PREFACE: BASICS OF THE METAVERSE

Dear Readers,

We are proud to present to you the 16th issue of the *Cyberpolitik Journal*. It is a great honor for all of us to continue our journey that we started eight years ago without interruption. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this domain within our limitations.

In an era dominated by the omnipresence of technology and interconnected digital ecosystems, the role of digital citizenship education cannot be overstated. The articles featured in the 8th volume and 16th issue of the *Cyberpolitik Journal* bring forth a compelling narrative, shedding light on diverse facets of cyber landscapes, from cybersecurity policies to geopolitical rivalries in cyberspace. Among these, the exploration of "Human Rights-Based Digital Citizenship Education" by Nezir Akyeşilmen stands out as a beacon, advocating for ethical considerations that pave the way for cyber peace.

The interconnectedness of our world has given rise to a digital society where the boundaries between physical and virtual realms blur. As such, fostering responsible digital citizenship is not merely an educational endeavor but a prerequisite for cultivating a global culture of cyber peace. Akyeşilmen's emphasis on human rights as the cornerstone of digital citizenship education is timely and resonates with the growing need to address the ethical dimensions of our online existence. The author develop and propose a human rights-based model for digital citizenship education that claiming ethics as the backbone of cyber peace. The article focuses on the basic elements of digital citizenship education and develops principles of education model from internationally recognized human rights instruments.

In the contemporary geopolitical landscape, cyber threats and attacks transcend national borders, making it imperative for nations to collaboratively address the challenges posed by the digital domain. The comparison of cybersecurity policies between Türkiye and England, as articulated by Gül Nazik Ünver, provides valuable insights into the diverse approaches



adopted by nations in fortifying their cyber defenses. National Cybersecurity strategies of Türkiye and England diverse but they have also many commonalities. International cooperation is a vital strategy for a successful cyber defence in cyberspace.

Akyeşilmen's proposition of a human rights-based approach to digital citizenship education urges us to consider the ethical implications of our actions in the digital realm. As we witness the fierce competition between major players like the United States and Russia in cyberspace, as presented by Gizem Dede, it becomes evident that a shared understanding of ethical behavior in the digital realm is essential for fostering trust and cooperation on the international stage. Dede, focuses mainly on cyber attacks by Russia but it is well known that all actors in cyberspace are pro offense in digital realm.

Elif Güldal Limon's exploration of Turkey's military communication systems highlights the critical role of cybersecurity and the imperative of localizing capabilities in the face of evolving threats. It is within this context that digital citizenship education emerges not only as a tool for individual empowerment but as a collective defense mechanism against cyber threats that transcend borders.

In the realm of opinions, Yavuz Akdağ's perspective on Cyber-AI technology and international relations underscores the rapid advancements in technology and their profound impact on geopolitics. However, as we navigate this intricate landscape, E. Dilara Kılınc's focus on the problems of digital citizenship in the cyber world resonates strongly. The challenges posed by the digital realm extend beyond mere technological aspects; they encompass the very fabric of our society, demanding a comprehensive and ethical approach.

Kamil Tarhan's review of "Technology Ethics: A Philosophical Introduction and Readings" aligns with the call for a philosophical underpinning in our approach to digital world. It prompts us to delve into the ethical frameworks that guide our interactions in cyberspace, emphasizing the need for a holistic understanding that goes beyond technical proficiency.

In conclusion, the 8th volume and 16th issue of the Cyberpolitik Journal offers a comprehensive panorama of the challenges and opportunities presented by the digital era. In this landscape, digital citizenship education emerges as a linchpin for cultivating responsible



behavior, fostering ethical considerations, and ultimately contributing to the attainment of cyber peace. As we navigate the complexities of cyberspace, it is essential to recognize that the path to a secure and harmonious digital future begins with the education of responsible and ethically conscious digital citizens.

EDİTORYAL ÖNSÖZ: METAVERSİN TEMELLERİ

Sevgili okuyucular,

Cyberpolitik journal Dergisi'nin 16. sayısını sizlere sunmaktan gurur duyuyoruz . Sekiz yıl önce başladığımız yolculuğumuzun kesintisiz devam etmesi hepimiz için büyük bir onur. Dijital dünya her geçen gün büyürken, yeni gelişmeler ve yeni teknolojiler ortaya çıkarken, biz de bu alanı kendi sınırlarımız dahilinde okumaya, anlamaya çalışıyoruz.

Teknolojinin ve birbirine bağlı dijital ekosistemlerin her yerde mevcut olduğu bir çağda, dijital vatandaşlık eğitiminin rolü yadsınamaz. *Cyberpolitik Journal*'ın 8. cildi ve 16. sayısında yer alan makaleler, siber güvenlik politikalarından siber uzaydaki jeopolitik rekabetlere kadar siber ortamın farklı yönlerine ışık tutan ilgi çekici bir anlatıyı ortaya koyuyor. Bunlar arasında Nezir Akyeşilmen'in "İnsan Hakları Temelli Dijital Vatandaşlık Eğitimi: Siber barış için etik" araştırması, siber barışın yolunu açacak etik hususları savunan bir yol gösterici rehber olarak öne çıkıyor.

Dünyamızın birbirine bağlılığı, fiziksel ve sanal alanlar arasındaki sınırların bulanıklaştığı dijital bir toplumun ortaya çıkmasına neden oldu. Bu nedenle, sorumlu dijital vatandaşlığın teşvik edilmesi yalnızca eğitimsel bir çaba değil, aynı zamanda küresel bir siber barış kültürünün geliştirilmesi için bir ön koşuldur. Akyeşilmen'in dijital vatandaşlık eğitiminin temel taşı olarak insan haklarına yaptığı vurgu günceldir ve çevrimiçi varoluşumuzun etik boyutlarına yönelik artan ihtiyaçla örtüşmektedir. Yazar, etiğin siber barışın omurgası



olduğunu iddia eden dijital vatandaşlık eğitimi için insan haklarına dayalı bir model geliştirip önermektedir. Makale, dijital vatandaşlık eğitiminin temel unsurlarına odaklanmakta ve uluslararası kabul görmüş insan hakları belgelerinden eğitim modelinin ilkelerini geliştirmektedir.

Çağdaş jeopolitik ortamda siber tehditler ve saldırılar ulusal sınırları aşıyor ve bu da ulusların dijital alanın yarattığı zorlukları işbirliği içinde ele almasını zorunlu kılıyor. Gül Nazik Ünver'in dile getirdiği Türkiye ve İngiltere siber güvenlik politikaları karşılaştırması, ulusların siber savunmalarını güçlendirmek için benimsedikleri farklı yaklaşımlar hakkında değerli bilgiler sağlıyor. Türkiye ve Endland'ın ulusal siber güvenlik stratejileri farklılık gösterse de pek çok ortak noktaya da sahiptir. Uluslararası işbirliği, siber uzayda başarılı bir siber savunma için hayati bir stratejidir.

Akyeşilmen'in dijital vatandaşlık eğitimine insan hakları temelli bir yaklaşım önerisi, bizi dijital alandaki eylemlerimizin etik sonuçlarını düşünmeye sevk ediyor. Gizem Dede'nin de belirttiği gibi, siber uzayda ABD ve Rusya gibi büyük oyuncular arasındaki şiddetli rekabete tanık olduğumuzda, uluslararası alanda güven ve işbirliğini geliştirmek için dijital alanda ortak bir etik davranış anlayışının gerekli olduğu açıkça ortaya çıkıyor. Dede, ağırlıklı olarak Rusya'nın siber saldırılarına odaklanıyor ancak siber uzaydaki tüm aktörlerin dijital alanda da suç yanlısı olduğu biliniyor.

Elif Güldal Limon'un Türkiye'nin askeri iletişim sistemlerini incelemesi, siber güvenliğin kritik rolünü ve gelişen tehditler karşısında yeteneklerin yerelleştirilmesinin zorunluluğunu vurguluyor. Bu bağlamda dijital vatandaşlık eğitimi sadece bireysel güçlendirme aracı olarak değil, sınırları aşan siber tehditlere karşı kolektif bir savunma mekanizması olarak da ortaya çıkıyor.

Görüşler açısından Yavuz Akdağ'ın Siber-Yapay Zeka teknolojisi ve uluslararası ilişkilere bakış açısı, teknolojideki hızlı gelişmelerin ve bunların jeopolitik üzerindeki derin etkisinin altını çiziyor. Ancak bu karmaşık manzarada ilerlerken E. Dilara Kılınç'ın siber dünyadaki dijital vatandaşlık sorunlarına odaklanması güçlü bir şekilde yankılanıyor. Dijital dünyanın getirdiği zorluklar salt teknolojik boyutların ötesine uzanıyor; kapsamlı ve etik bir yaklaşım gerektiren toplumumuzun dokusunu kapsıyorlar.



Kamil Tarhan'ın "Teknoloji Etiği: Felsefi Bir Giriş ve Okumalar" incelemesi, dijital dünyaya yaklaşımımızda felsefi bir temel oluşturma çağrısıyla örtüşüyor. Teknik yeterliliğin ötesine geçen bütünsel bir anlayışa duyulan ihtiyacı vurgulayarak bizi siber uzaydaki etkileşimlerimize yön veren etik çerçeveleri araştırmaya teşvik ediyor.

Sonuç olarak Cyberpolitik Dergisi'nin 8. cildi ve 16. sayısı, dijital çağın sunduğu zorlukların ve fırsatların kapsamlı bir panoramasını sunuyor. Bu ortamda dijital vatandaşlık eğitimi, sorumlu davranışı geliştirmek, etik hususları teşvik etmek ve sonuçta siber barışın sağlanmasına katkıda bulunmak için bir temel taşı olarak ortaya çıkıyor. Siber uzayın karmaşıklıklarında yol alırken, güvenli ve uyumlu bir dijital geleceğe giden yolun sorumlu ve etik açıdan bilinçli dijital vatandaşların eğitimiyle başladığını kabul etmek önemlidir.

Nezir AKYEŞİLMEN, Ph.D

Editor-in-Chief

x

