Politics and Governance
2025 • Volume 13 • Article 10218
https://doi.org/10.17645/pag.10218

ARTICLE

Open Access Journal

The Social Movement Evolution of Non-State Armed Groups in the Web 3.0 Era

Yaohui Wang † and Yang Qiu †

Zhou Enlai School of Government, Nankai University, China

† The two authors contributed equally to this article and therefore share co-first authorship

Correspondence: Yang Qiu (yang.qiu12@mail.nankai.edu.cn)

Submitted: 27 February 2025 **Accepted:** 18 September 2025 **Published:** 27 November 2025

Issue: This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

Abstract

How do the emerging Web 3.0 technologies affect the survival of non-state armed groups (NSAGs) in their violent struggles vis-à-vis state entities? While techno-optimists argue that Web 3.0 can democratize the internet and curb monopolistic practices, its decentralized features, such as enhanced privacy, data ownership, and personalization, also present significant security challenges. These technologies can be weaponized by NSAGs to promote their efficiency and resilience. Borrowing insights from social movement theory, we construct a theoretical framework to explain how Web 3.0 applications affect the dynamics of NSAGs by impacting their organizational modes and strategies. It is argued that blockchain-based platforms, metaverse projects, and other Web 3.0 technologies promote the efficiency of the recruitment, training, financing, purchasing, and communication processes of NSAGs, increasing their capacities as social organizations, and thereby render these groups more resilient to collapse. We illustrate and corroborate our theoretical claims by examining the cases of how NSAGs such as the Islamic State utilize decentralized crypto exchanges and the Dark Web in their operations.

Keywords

blockchain; cryptocurrency; non-state armed groups; Web 3.0

1. Introduction

Over the past several decades, a growing consensus has emerged among scholars and industry experts that the rise of Web 3.0 represents a transformative force poised to revolutionize digital life (Barassi & Treré,

2012; Lassila & Hendler, 2007). In contrast to the Web 2.0 era, where powerful internet conglomerates dominate the digital landscape, Web 3.0 promises to decentralize control and empower users. During the contemporary Web 2.0 age, tech giants such as Facebook and Amazon wield unprecedented influence over the digital ecosystem, compelling users to rely on their proprietary platforms and algorithms. This dominance not only stifles competition from smaller innovators but also enables giant corporations (e.g., Facebook and Amazon) to amass vast amounts of user data, which they leverage to maximize profits and shape online behavior. Importantly, this practice significantly increases the risk of data leaks and illicit data manipulation for political objectives. In the infamous Facebook–Cambridge Analytica data scandal, for instance, whistleblowers revealed that approximately half a billion Facebook users' profile data had been secretly harvested to manipulate US presidential election outcomes (Cadwalladr & Graham-Harrison, 2018; Hinds et al., 2020). Indeed, one can argue that the integrity of democratic governance and the preservation of civil liberties may be significantly undermined by these big techs' interferences.

Thanks to recent advancements in internet technology, Web 3.0—the third generation of the internet—appears poised to address and potentially eliminate these concerning abusive practices. Cutting-edge technologies, particularly blockchain, cryptocurrencies, generative AI tools (such as ChatGPT and Sora), and the metaverse, have brought the foundational structure of the internet to a critical juncture of transformation. These innovations empower web users to maintain ownership of their data, effectively merging their roles as internet consumers and profit generators. This integration transforms consumption and production into a unified process, redefining the dynamics of digital interaction (Hyzen, 2023). In this way, the Web 3.0 trend not only enhances web users' financial gains but also curbs the dominance of powerful centralized corporations and their associated mega-platforms over the internet ecosystem. This shift fosters a more decentralized, personalized, and resilient digital environment, less susceptible to top-down interference. As highlighted by a policy paper published by the Tony Blair Institute for Global Change, Web 3.0 "would mark a departure from the centralized mega platforms and corporations that dominate the ecosystem currently and, proponents claim, fix what's wrong with the internet of today along with reversing the erosion of democracy" (Johnson, 2022).

Despite these advanced technological innovations, a small but increasing number of scholars and policymakers have begun to voice concerns about the potential challenges posed by Web 3.0 technologies. Professionals in STEM (Science, Technology, Engineering, and Mathematics) fields argue that while Web 3.0 may disrupt the existing power asymmetry between large corporations and individual users, it also introduces a range of cybersecurity threats, including fraud and the theft of user information (Bharadiya, 2023). Flash loan attacks, for example, are an increasingly frequent type of exploitation that takes place in decentralized finance (DeFi) ecosystems—operators utilize uncollateralized lending to carry out attacks. On May 12, 2021, for example, cyberthieves perpetrated a strike against the DeFi protocol xToken and took away USD 24.5 million (Copeland, 2021). The severity of these crimes is particularly concerning, as users themselves may now bear the responsibility for safeguarding their own data, making them potentially accountable for any breaches or losses.

Unsurprisingly, these novel forms of crime have led some scholars to highlight the unprecedented complexity of cybercrime in the Web 3.0 era. Zuo (2023) argues that the decentralization and anonymity features of Web 3.0 may provide illicit actors with opportunities to evade government regulations, particularly in activities such as underground fundraising and money laundering. Vayadande et al. (2024)

note that the decentralized nature of Web 3.0 poses significant challenges for account recovery, because the loss of internet keys in this new era is likely to be irreversible. Additionally, Zhu et al. (2024), utilizing survey methods, find that the technical barriers for users adapting to the Web 3.0 ecosystem can be prohibitively high. They also emphasize that effective online identity management becomes particularly challenging, as users no longer rely on traditional usernames and passwords to establish their digital identities. In a recently published article, O'Brien (2023) outlines several security concerns associated with Web 3.0, including smart contract vulnerabilities, private key management issues, phishing and scams, and the lack of user-friendly interfaces. O'Brien (2023) notes that these concerns "must be addressed to ensure a safe and secure Web3 ecosystem for all stakeholders involved." Outside academia, there have also been increasing doubts cast on the utility of the Web 3.0 movement. Elon Musk, the founder, CEO, and chief engineer of SpaceX, and Jack Dorsey, the chairman of payments company Block, for example, both assert that there is an urgent need to put the brakes on the momentum around the Web 3.0 trend (Shead, 2021).

While the Web 3.0 trend has gained significant prominence in STEM fields and industrial sectors, there remains a notable gap in the political science literature regarding the political risks associated with these advanced technologies. For instance, to what extent, and through which causal mechanisms, does Web 3.0 influence the use of political violence by non-state actors? Given that Web 3.0 has the potential to fundamentally reshape the online landscape, it raises the question of whether political actors seeking to consolidate and expand their power might also exploit these technologies. If so, how does Web 3.0 impact the strategies employed by these actors? Despite the clear importance of understanding the relationship between Web 3.0 and political violence, there has been a striking lack of political science research dedicated to exploring these puzzles.

To address this research gap, this article seeks to bridge existing scholarship on the security challenges posed by Web 3.0 with political science research on non-state armed groups (NSAGs). The focus here is specifically on NSAGs, as they are generally at a military disadvantage compared to nation-states (Podder, 2013). Consequently, these groups are likely to have strong incentives to conceal their operations by operating underground. This aligns with the core feature of Web 3.0—decentralization—which suggests that Web 3.0 technologies may exert a particularly significant influence on the organizational structures and strategies of NSAGs.

Drawing on insights from social movement theory, this article investigates the channels through which cutting-edge Web 3.0 technologies enable NSAGs to function more effectively and resiliently as social organizations. Specifically, it argues that Web 3.0 applications, such as blockchain-based platforms, metaverse projects, and decentralized data storage, simultaneously enhance the recruitment, training, purchasing, financing, and communication processes of NSAGs, thereby rendering these groups more decentralized and better equipped to confront their rivals. Here, it should be carefully noted that NSAGs typically refer to domestic and transnational resistant organizations, rebel groups, and insurgent groups (Englehart, 2016). In this article, however, we deliberately avoid using these more conventional terms, as they are often criticized for being overly subjective, politicized, and weaponized by Western political actors to delegitimize their opponents (LeVine, 1995). Therefore, we opt to use the term NSAG as a more neutral and technical designation.

The remainder of this article is structured as follows. First, we provide a comprehensive review of the background and characteristics of the Web 3.0 trend. Second, drawing on social movement theory, we

propose a causal mechanism to explain how these advanced technologies influence the organizational structures and strategies of NSAGs. Next, we conduct empirical analyses to illustrate and validate our theoretical claims, using two qualitative case studies on the use of cryptocurrencies and the Dark Web by NSAGs. Finally, we offer concluding remarks and discuss the policy implications.

2. A Review of the Development of Web 3.0 Technologies

Web 3.0, often referred to as the semantic web or decentralized web, is regarded as a significant milestone in the historical development of network technology (Nasar, 2023). Web 3.0 is defined by decentralization and user sovereignty, with core technologies like blockchain and cryptocurrencies enabling its functionality, while auxiliary innovations such as non-fungible tokens (NFTs) and DeFi expand its practical applications. In the Web 3.0 era, users no longer need to create multiple identities across different centralized platforms; instead, they can establish a single, decentralized universal digital identity system that operates across various platforms. Given the technical complexity of Web 3.0 technologies, it is essential to first provide a brief overview of the development from Web 1.0 to Web 3.0 before presenting our theoretical framework.

2.1. The Internet System Before Web 3.0 (1989–2013)

Historically, the internet has gradually evolved from Web 1.0 to Web 3.0. During the Web 1.0 era, information access was one-directional as users could only retrieve static content updated solely by webmasters, leaving them passive network nodes without interactive capacity (Tekdal et al., 2018). The business model was equally restrictive, relying primarily on click-through rates, with profit dependent solely on the frequency of user clicks. This model persisted until the turn of the millennium, when the emergence of Web 2.0 prompted leading network companies to shift their focus toward portal sites.

Although coined in the 1990s, the term "Web 2.0" only attracted much attention after the O'Reilly Media Web 2.0 Conference in 2004 (Prandini & Ramilli, 2012). Conceptually, Web 2.0 is characterized by the widespread use of mobile internet technologies, fostering a user-centric and collaborative environment (Jacksi et al., 2020). In this era, users could not only search and review information but also act as content providers and interact with other users. Unlike Web 1.0's static platforms for texts, images, and videos, Web 2.0 enabled multidimensional information exchange, significantly enhancing user experience.

2.2. The Contemporary Web 3.0 Era

The evolution from Web 2.0 to Web 3.0 marks a significant milestone in the history of the online world. The defining characteristic of Web 3.0 is the effective interconnection between users, facilitating the creation of user profiles (Jacksi, 2019). In comparison to Web 2.0, which often failed to reflect netizens' values, Web 3.0 introduced a new, decentralized ecosystem that shifts resources from large tech companies to individuals. This transition brought three key features: user interactions and personalized experiences, the rise and widespread adoption of virtual currencies and exchanges, and the growing recognition of the internet's value alongside demands for financial security (Rathor et al., 2023). Fundamentally, Web 3.0 rests on ideological rather than purely technological innovation.

On a macro level, Web 3.0 represents the current phase of the internet ecosystem—an increasingly "decentralized" online world driven by blockchain technology. Online content providers can now interact seamlessly across different websites, enabling more efficient information integration and freer flow of digital assets through decentralized platforms. Users can now access various nodes without compromising their data. Most notably, there has been a rise in Web 3.0 applications that allow users to input labor values and generate revenue from their digital assets (data). Data created by users are synchronized instantaneously across the internet (Kurilovas et al., 2014), making data inherently decentralized, interconnected, and structured for easier storage and use. This more personalized form of data creation and transfer enhances users' ability to communicate and access information.

Web 3.0 incorporates the concept of the semantic web, linking data across web pages to enable more efficient information comprehension and utilization, intelligent search, and data-understanding capabilities. In this way, the semantic web allows computers to better understand human languages and intentions. By promoting open standards, interoperability, and system flexibility, Web 3.0 fundamentally transforms both the mechanisms of individual online interactions and the business models of web companies (Murray et al., 2023).

2.3. Main Types of Web 3.0 Application Technologies

There are over 20 types of Web 3.0 application technologies, including blockchain, smart contracts, decentralized storage, artificial intelligence (AI), encryption, distributed storage, big data, cloud computing, and the Internet of Things (IoT). Specifically, blockchain, smart contracts, encryption, and the IoT are closely tied to online transactions, digital currencies, and digital finance (Wan et al., 2024).

Blockchain technology, perhaps the most well-known of Web 3.0 technologies, embodies the core operational characteristics of Web 3.0: decentralization, security, and transparency (Zhang et al., 2023). It ensures the security and consistency of data by storing transaction information in record boxes (blocks) and linking multiple blocks to form a chain structure within peer-to-peer (P2P) networks, thereby providing a reliable platform for transactions and data storage. Additionally, smart contracts, self-executing computer programs that operate on the blockchain, are particularly relevant for businesses like digital asset management. Similarly, encryption technology, a critical security feature of Web 3.0, is used to protect user privacy and secure transaction information. Finally, the IoT is an indispensable component of Web 3.0. In the Web 3.0 era, the IoT not only facilitates the connection of different devices but is also integrated with blockchain, AI, and other technologies to deliver more efficient, secure, and intelligent internet services. As a result, the IoT plays a pivotal role in Web 3.0, especially in areas such as privacy protection, digital currencies, and digital finance. See Figure 1 for a visualization of Web 3.0 application technologies.

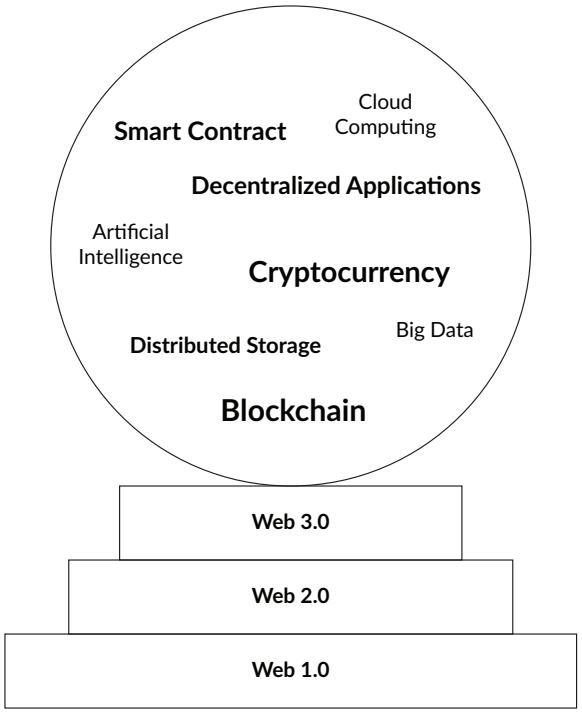

Figure 1. Main types of Web 3.0 application technologies. Note: Web 3.0 application technologies vary in prevalence, so the more commonly used ones are shown in larger font.

3. NSAGs in the Web 3.0 Era: A Social Movement Perspective

While the political actions of NSAGs can be aggressive and intimidating, a surprising scholarly consensus holds that these groups are, in fact, quite vulnerable, as they are inherently subject to risks of internal dysfunction (McLean et al., 2018; Vittori, 2009). From a political sociology perspective, NSAGs are not fundamentally different from legitimate, non-violent social groups—such as environmental NGOs, yoga clubs, athletic teams, and music bands. Regardless of their aims or scope, all such groups need well-designed organizational structures and secure resources to survive and sustain themselves. In this sense, like all other social organizations, NSAGs must first and foremost function as organizations: NSAGs must recruit members, propagate their political ideologies, secure stable and protected spaces in which to undertake their activities, establish effective communication channels, and raise funds (Wang et al., 2022).

Furthermore, in their struggle against nation-states, NSAGs must also engage in activities such as purchasing and transporting weapons and equipment, and maintaining confidentiality to evade government crackdowns (Jacobson, 2010). Unsurprisingly, the political science literature has consistently shown that most NSAGs have notably short lifespans and often fail to achieve their intended objectives. For example, early quantitative studies by Rapoport (1983) found that approximately 90 percent of certain types of NSAGs do not survive their first year, and of those that do, 50 percent do not last more than a decade. More recent empirical studies suggest that Rapoport's (1983) estimate may be overly pessimistic, but they nonetheless confirm the broader finding that most NSAGs are inherently short-lived (McLean et al., 2018).

Despite the conventional wisdom that NSAGs are unlikely to survive for long or achieve their objectives, this observation may be subject to revision in the context of the contemporary Web 3.0 era. Conceptually,

the decentralization inherent in Web 3.0 could inadvertently empower NSAGs, especially those seeking to conceal their operations from their adversaries—nation-states and rival governments. As such, this logic raises a crucial theoretical and policymaking question: How do Web 3.0 technologies impact the operations and internal functions of NSAGs? In other words, how and through what mechanisms does Web 3.0 influence the organizational structures and strategies of NSAGs? To address this question, we draw on insights from social movement theory within the field of sociology to construct a comprehensive analytical framework.

3.1. A Social Movement Theory of NSAGs

Across various fields of social science, there has been abundant literature on the formation, development, and impact of social organizations (Morris, 2000). Yet, the research to date has been characterized by a distinct lack of knowledge on how NSAGs function as social organizations. In this regard, social movement theory is uniquely well-positioned to serve as the theoretical ground for our conceptual framework, which examines the dynamics of NSGAs in the Web 3.0 era, inasmuch as the theory places a particular emphasis on the micro-level elements that constitute the political mobilizations of the violent actors. As famously put by Beck (2008) nearly two decades ago, "[social movement theory] sees tactics, movements, and actors arrayed along a spectrum of related phenomenon rather than boxed in by formal, discrete categories" (p. 1566). Thus, before presenting our analytical framework, we first offer a brief review of the key concepts that have shaped social movement theory over the past 40 years.

Social movement theory is a school of sociological thought that examines the processes behind social movements. While it is true that numerous factors contribute to the dynamics of social groups, this does not necessitate a lengthy list of control variables. Rather, the focus should be on identifying the most fundamental variables that directly shape collective social actions. As such, social movement theory has predominantly concentrated on three key variables: (a) the framing process (perception, interpretation, and cognitive attribution) of political affairs; (b) mobilizing resources; and (c) political opportunities. Originating in the US and Western Europe over the past several decades, this threefold framework aims to explain when and how social movements emerge and evolve (Beck, 2008).

The first array of the tripartite model emphasizes the rhetorical and symbolic elements in social collective actions, which, as noted by McAdam (2017), are "the shared meanings and cultural understandings that people bring to any instance of potential mobilization" (p. 194). Logically, for a political movement to gain public endorsement, it needs to echo some widespread pre-existing sentiments among the general population. The sense of grievances, in this regard, often stands out as a pivotal magnet to attract people's support for NSAGs, because the organizers need to construct strategic narratives and frame political violence in a way that significantly resonates with some shared values in society (Ghatak et al., 2019). In doing so, organizers strive to convince disgruntled citizens and would-be fighters that the key solution to redress the problem they face is to act in groups and participate in violent campaigns. In this process, the media and other propaganda tools are important channels for NSAGs to disseminate their doctrines (rhetoric and claims) and recruit fighters. Indeed, framing has long been a major organizational effort in many NSAGs such as al-Qaeda, the Islamic State of Iraq and Syria (ISIS), and South American narco-NSAGs.

Second, the leadership of NSAGs needs to take control of mobilizing resources in order to sustain collective actions (Jenkins, 1983). By mobilizing resources, we refer to both tangible (funds, weapons, equipment) and

intangible resources such as training, transportation, and communication methods. Financing, in particular, is a critical material component for NSAGs (Freeman & Ruehsen, 2013). Here, it is worth noting that political violence is a costly venture. For NSAG organizers, securing reliable financial channels is crucial to purchasing arms and intelligence, paying bribes to corrupt officials, propagating their ideologies, and carrying out violent operations. Without these resources, NSAGs would be unable to function as organizations and would struggle to survive under government crackdowns.

The final pivotal factor that directly impacts the success or failure of NSAGs is the political opportunity external to the groups (Suh, 2001). Political opportunity, in this context, refers to sudden changes that dramatically alter the general environment for NSAGs, particularly events that shift the balance of power between NSAGs and the government in favor of the former. These shocks may include war, international sanctions, fiscal crises, changes in political leadership, natural disasters, and major technological innovations, among others. In the absence of political opportunities, governments typically hold an unbalanced advantage over non-state organizations, making it easier to eliminate NSAGs. However, sudden political shocks can instantly alter the bargaining structure, providing a unique "window of opportunity" for challengers (Meyer & Staggenborg, 1996). Thus, the likelihood of success in organizing collective actions can be significantly increased for certain movements shaped by the broader international and domestic political environment.

3.2. How Web 3.0 Technologies Impact the Organization of NSAGs: A Theoretical Framework

Based on social movement theory, Web 3.0 technologies directly impact the organizational modes and strategies of NSAGs, mostly on three aspects: (a) perception, interpretation, and cognitive attribution, (b) mobilization of resources, and (c) propaganda and communications. Taken together, these aspects construct political opportunities for NSAGs to survive and proliferate. For concreteness, we visualize our theoretical framework in Figure 2.

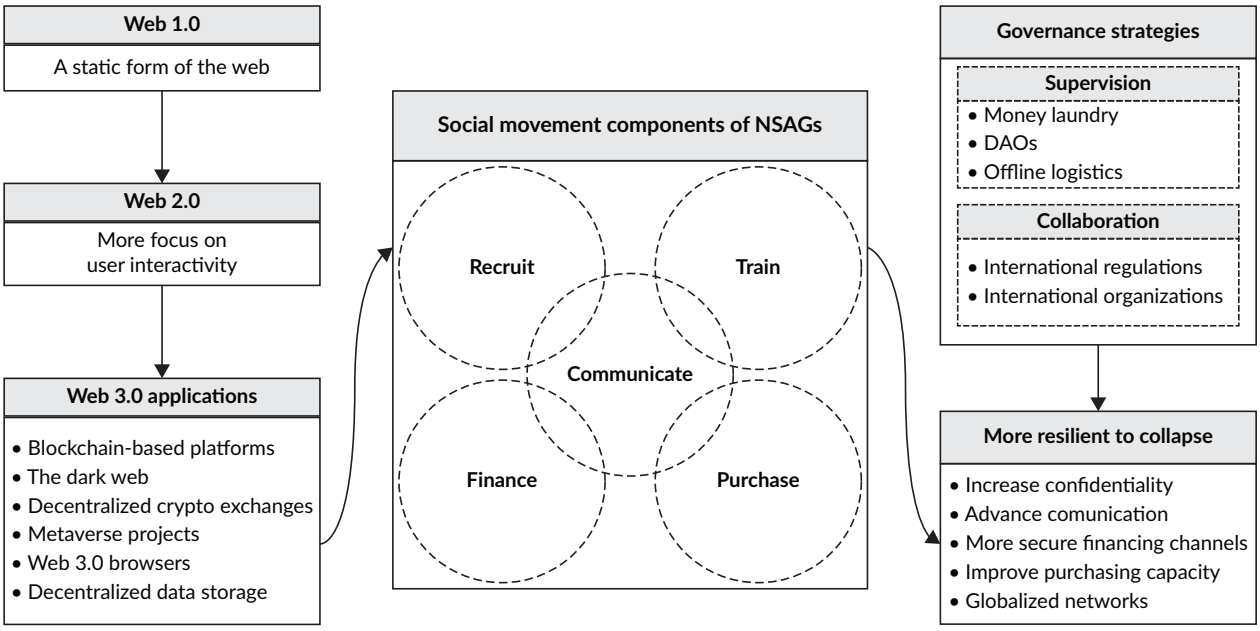

Figure 2. A social movement model of NSAGs in the Web 3.0 era. Note: DAOs = Decentralized Autonomous Organizations.

Firstly, leveraging their powerful transmission capacity, encrypted networks can influence the perception, interpretation, and cognition of NSAG members and potential recruits. This transmission process involves communication, the formation of ideological beliefs and action goals, the pursuit of recognition, and the promotion of training. Such processes can evoke resonance among netizens, who may then support the values of NSAGs. In the Web 3.0 era, NSAGs often seek to gain citizens' emotional endorsement through cyber technologies. By utilizing encrypted chat rooms and communication systems, NSAGs spread and infiltrate their violent ideologies, seeking both material and spiritual support from netizens. Scholarly works have demonstrated that some NSAG campaigns in sub-Saharan Africa exploit Web 3.0 applications to convey messages to potential fighters. For example, al-Shabaab in Somalia utilizes encrypted networks to deploy its fighters (Pearlman & Cunningham, 2012). Al-Shabaab is an Islamic fundamentalist NSAG primarily operating in Somalia, but also active in the broader East African region. Historically, the group has expressed support for Osama bin Laden and al-Qaeda. Despite bin Laden's death, al-Shabaab has continued launching attacks in Kenya, Libya, and Uganda, and has murdered numerous civilians, particularly women and children. Their violent campaign targets the Somali government and the African Union, and the group controls a significant portion of territory in south-central Somalia. Similarly, encryption technologies are embedded in the daily communication of ISIS, primarily through Web 3.0 apps. ISIS fighters have been known to download these apps onto their devices to store and exchange NSAG-related information. In some lone wolf attacks, there is evidence that NSAGs have used Web 3.0 apps for communication. For instance, Anwar al-Awlaki, a member of al-Qaeda, collaborated with Rajib Karim, a British Airways employee, to set up an encrypted communication system for planning attacks on British Airways (Dodd, 2011).

Second, extensive studies have shown that NSAGs use cryptocurrencies to finance their operations. Theoretically, NSAGs can generate resources through both external and internal channels. External channels typically include state sponsorship, while internal channels often involve taxation, public donations, and kidnapping. Regardless of the sources of financing, NSAGs must secure stable channels to collect resources and make payments when purchasing intelligence or equipment. With the rise of Web 3.0 technologies, cryptocurrencies have become a major financing tool for NSAGs. Since cryptocurrencies offer anonymity and untraceability for monetary transactions, they are highly favored by NSAGs, who use Bitcoin and other open-source P2P currencies for transactions. For example, ISIS, which has seen its traditional revenue sources such as oil and taxes diminish in recent years, now relies on cryptocurrencies like Bitcoin, Dash, Ethereum, Monero, Verge, and Zcash for a significant portion of its financial assets. Similarly, al-Shabaab, the NSAG mentioned earlier, has also begun to use cryptocurrencies to raise funds and make payments. Hassan Afgooye, a member of al-Shabaab's leadership, oversees a complex financial network based primarily on cryptocurrencies. This network raises funds through fake charities, extortion, and kidnapping, which are then converted into cryptocurrencies. Afgooye uses these funds to support al-Shabaab's violent campaign (U.S. Department of the Treasury, 2022).

Third, propaganda based on Web 3.0 technologies has become central to how NSAGs function as organizations. For decades, NSAGs have sought effective online propaganda tools to convey their messages to the general public, and the development of Web 3.0 applications in recent years has accelerated the weaponization of these cutting-edge technologies. According to scholarly findings, many Web 3.0-based Dark Web platforms and online chatrooms are connected to NSAGs, which often post extremist speeches by their leaders or senior members to propagate violent ideologies (Rusumanov, 2016). For example, both al-Shabaab and Boko Haram have been active on Web 3.0-based Dark Web platforms, using them to sustain

public advocacy and coordinate financial activities to ensure adequate funding. These speeches often justify the excessive use of force, arguing that such actions are righteous if their goals are deemed justified (Rusumanov, 2016). Specifically, NSAGs often employ AI models to generate deepfake content, creating seemingly authentic images and videos to spread their extremist ideologies and convince audiences. In doing so, NSAGs contribute to misinformation, division, and political turmoil among their target populations. In effect, ISIS carried out a deadly attack in Moscow in March 2024, using Web 3.0 technologies to deploy members and materials. The Russian government found evidence that ISIS funded the attack through cryptocurrency transactions and the Dark Web, enabling them to carry out the operation (Huang, 2025).

Taken together, the Web 3.0 technologies discussed above directly impact the organizational modes and strategies of NSAGs, enabling them to survive and operate as social organizations. These technologies facilitate more efficient communication, recruitment, incitement, and propaganda, while also providing clandestine channels for weapons procurement and unregulated financial transactions.

4. Case Studies: NSAGs' Engagement With Web 3.0 Technologies

To corroborate and illustrate our theoretical claims, we employ two case studies. The first examines how NSAGs exploit AlphaBay, a notorious Web 3.0-based Dark Web platform, for communication, propaganda, recruitment, member training, and financial transactions. The second case study focuses on how Web 3.0 technologies influence the financing strategies of ISIS, with particular attention to its use of cryptocurrencies for resource collection and payments.

4.1. Dark Web Transactions and AlphaBay

In recent decades, the Dark Web has become a crucial platform for NSAGs to plan and execute violent attacks (Sageman, 2011). Technically, the Dark Web is a subset of the Deep Web, which itself is part of the broader World Wide Web—the publicly accessible internet. Due to its clandestine nature, the Dark Web can only be accessed through specialized software, unique licenses, or specific computer settings. In the Web 3.0 era, the Dark Web's characteristics have been significantly enhanced, as the development of decentralized technologies has further bolstered the anonymity of its users.

In particular, Web 3.0 utilizes decentralized protocols that prioritize individual privacy and resist internet censorship, aligning perfectly with the core characteristics and functions of the Dark Web. As a result, new decentralized marketplaces, forums, and chatrooms have emerged within the Dark Web, facilitated by Web 3.0 technologies. Consequently, NSAGs are increasingly relying on the Dark Web, viewing it as a secure and reliable space that is largely impervious to government crackdowns.

Since the Dark Web operates within the underworld of the regular internet, users need special "keys" to access it, namely the anonymous proxy tool Tor, or "The Onion Router." Tor protects users in a way similar to the layers of an onion, ensuring that their addresses, identities, and the websites they visit remain completely anonymous (Montieri et al., 2018). Paul Syverson, the mathematician from the U.S. Naval Research Laboratory who invented Tor, originally designed the tool to safeguard the privacy of law-abiding individuals (Reed et al., 1998). However, its unintentional benefit has been to support NSAGs. For instance,

Bitcoin, a cryptocurrency frequently traded on the Dark Web, allows NSAGs to conduct financial transactions without relying on credit cards or bank accounts, enabling them to evade government oversight.

Given that the Dark Web offers a safe haven for users to evade government supervision, it has become a hub for numerous illicit activities, including arms deals, drug trafficking, pornography, and financial fraud. For NSAGs, in particular, the Dark Web serves as a crucial underground channel for recruiting members, purchasing weapons, propagating ideologies, and plotting violent attacks. Specifically, NSAGs use chatrooms to spread extremist ideologies, recruit new members, and establish "master-slave" relationships within their networks. Both ISIS and al-Qaeda, for example, are known to utilize the Dark Web to recruit foreign terrorist fighters and organize attacks. Despite global efforts to crack down on these dangerous networks, encrypted communications remain largely impenetrable. Research has shown that ISIS and other jihadist groups have long relied on encrypted mobile apps, such as Telegram, to exchange sensitive information (Bloom et al., 2019; Shehabat et al., 2017). Additionally, these groups often post lectures and tutorials to train their members on how to use the Dark Web effectively to evade government detection (Coker et al., 2015).

To illustrate, a prominent example is the case of AlphaBay. Since its establishment in 2014, AlphaBay facilitated nearly USD 1 billion in illegal transactions involving drugs, firearms, embargoed goods, stolen items, counterfeit products, malware, and NSAG-related activities. According to a RAND report, NSAGs could purchase materials like *The Terrorist's Handbook* and the *Explosives Guide* on AlphaBay (Ryan et al., 2017). Furthermore, the report highlights that AlphaBay also offered a fake documents service, which sold customized fake government-issued documents and passports to NSAGs. More broadly, the illicit activities of NSAGs on AlphaBay included a range of transactions that supported their operations.

First, the Dark Web serves as a platform for member recruitment, communication, and training. On the decentralized AlphaBay platform, NSAGs like ISIS were able to propagate extremist ideologies, recruit new members, allocate funding to followers, and purchase training materials, such as courses on bomb-making. To be more specific, one study by the European Union Institute for Security Studies notes that, on AlphaBay, ISIS sold manuals containing terrorist operational guidance and instructions for manufacturing explosives to jihadist sympathizers (Berton, 2015). Although AlphaBay was not intentionally designed as a communication outlet for NSAGs, its relative anonymity and security nevertheless offered such organizations a platform to disseminate training materials. Moreover, according to the study, AlphaBay's fake document services enabled jihadist members and sympathizers to obtain high-quality counterfeit IDs, allowing them to circumvent legal restrictions and border controls to enter Iraq and Syria (Berton, 2015). Again, such services of AlphaBay facilitated the recruitment and communication activities of NSAGs.

Second, AlphaBay facilitated fundraising and financial transactions. Similar to other Dark Web platforms, it provided NSAGs with secure channels to receive and redistribute digital currencies like Bitcoin (Dilipraj, 2014). On the one hand, with respect to fundraising, supporters of ISIS used Bitcoin (and other cryptocurrencies), transferred via trade or donations, to fund the terrorist organization (Berton, 2015). AlphaBay may have also provided NSAGs with additional sources of funding by selling stolen bank card information and hacked PayPal accounts, which could be exploited by NSAGs with minimal risk of detection by state authorities. On the other hand, with the funds obtained through AlphaBay, NSAGs were able to purchase essential resources for their survival and operations. Notably, AlphaBay's online markets sold computer hacking tools, firearms, and ammunition to groups like ISIS. As a matter of fact, when AlphaBay was taken down, there were over

100,000 listings for stolen documents, firearms, and other illicit goods (U.S. Department of Justice, 2017). All these underscore AlphaBay's significance as a conduit for financing and equipping NSAGs.

Third, AlphaBay was also involved in illicit drug trafficking. According to the U.S. Department of the Treasury (2024), AlphaBay and similar Dark Web platforms employ encryption technologies that shield communications and transactions from state monitoring. This makes them highly attractive to drug cartels, which exploit these sites both to market toxic chemicals and to acquire the raw materials and manufacturing equipment necessary for their production (U.S. Department of the Treasury, 2024). In July 2017, in an international law enforcement investigation, the U.S. Department of Justice took down AlphaBay, which at the time had evolved into one of the world's largest Dark Web platforms. According to a BBC report, approximately USD 450 million was spent on the marketplace between May 2015 and February 2017, with illegal drugs such as heroin and fentanyl listed for sale (Baraniuk, 2017). At the time of its takedown, AlphaBay hosted over 250,000 listings for illegal drugs and toxic chemicals (U.S. Department of Justice, 2017). To further illustrate the Dark Web's critical utility to their operations, take Mexican cartels such as Sinaloa as an example. These cartels exploit the Dark Web by using cryptocurrencies to purchase precursor chemicals and, after processing them into narcotics, relying on the same platforms to traffic drugs to American consumers. Such activities have further exacerbated the US opioid crisis, which claimed more than 107,000 American lives from overdoses in 2023 alone (U.S. Department of the Treasury, 2024).

4.2. ISIS's Use of Cryptocurrencies

For NSAGs, the ideal funding channels should possess six key characteristics: quantity, legitimacy, security, reliability, controllability, and simplicity (Freeman & Ruehsen, 2013). To this end, cryptocurrencies are frequently utilized by NSAGs such as ISIS in their financial activities.

Cryptocurrencies, built on blockchain technology, are typically more reliable and anonymous than conventional currencies. Technically, cryptocurrency can be understood as a medium of exchange that uses cryptographic principles to secure transactions and regulate the creation of transaction units. Bitcoin, introduced in 2009, was the first decentralized cryptocurrency. Unlike traditional banking systems, which depend on centralized regulatory frameworks, cryptocurrencies are based on a decentralized consensus mechanism. In the Web 3.0 era, cryptocurrencies serve as a medium of value exchange, facilitating payments for decentralized applications. Cryptocurrency exchanges in Web 3.0 play a crucial role in asset trading by enabling secure transactions through smart contracts, enhancing both security and transparency. With their decentralization, security, and financial autonomy, cryptocurrencies offer NSAGs an effective means of funding their violent operations. For instance, in January 2017, it was reported by Indonesia's financial transactions agency that Islamic militants in the Middle East used Bitcoin to support terrorist operations in the country (Yuniar, 2017). And in March 2024, the Islamic State – Khurasan Province, ISIS's affiliate in Afghanistan, carried out a terrorist attack in Moscow, partially financed using cryptocurrency ("Category deep-dive," 2025).

ISIS was one of the earliest NSAGs to employ cryptocurrencies. In addition to Bitcoin and Tether, recent evidence demonstrates that Monero has also become a new type of cryptocurrency used by ISIS to collect donation money from its sympathizers (Awasthi, 2024). In a recent policy analysis published by TRM Labs ("TRM finds mounting evidence," 2023), a reputable blockchain intelligence company, increasing ISIS funds

had been transferred using cryptocurrencies throughout Asia. In Tajikistan, most particularly, a number of pro-ISIS organizations raised approximately USD 2 million on Tron (a decentralized blockchain-based operating system) in 2022. These funds were spent on the recruitment of terrorists to join the Islamic State – Khurasan Province. Similarly, other reporters found that ISIS used Bitcoin to fund the bombings in Sri Lanka on April 21, 2019. Before the attack, ISIS used CoinPayments, a payment portal based in Canada, to convert its Bitcoin into paper currency. In March 2020, the US federal court sentenced Zoobia Shahnaz from Long Island, New York, to 13 years in prison for using Bitcoin and other cryptocurrencies to conduct money laundering for ISIS (Saravalle & Rosenberg, 2018). In addition, NSAGs also used social media to process cryptocurrency transactions. For example, in August 2015, Ali Shukri Amin, a 17-year-old from Virginia, US, was sentenced to 11 years in prison for publicly supporting ISIS on his Twitter account (Abutaleb & Cooke, 2016). Under the account name @Amreekiwitness, Ali Shukri Amin posted tutorials on how to use Bitcoin to fund ISIS and other NSAGs.

Several cases in 2015 revealed how ISIS sympathizers experimented with cryptocurrencies to provide material support to the organization. In January, Abu-Mustafa, a known ISIS supporter, successfully raised five Bitcoins (approximately USD 1,000 at the time) before the FBI intervened and shut down his account. This case is widely regarded as the first documented instance of ISIS employing cryptocurrency on the Dark Web. In May, another ISIS supporter dubbed "Abu Ahmed al-Raqqa" issued an appeal on the Dark Web, soliciting donations for ISIS in the form of Bitcoin. Later, in August, an ISIS-affiliated hacker attempted to extort two Bitcoins (roughly USD 500 at the time) from a US internet company, offering in return to remove a bug from their software. Beyond financial extortion, the hacker's far more damaging act was exploiting the internet company's bug to obtain the names of 1,351 US government and military personnel and sharing them with ISIS, which later compiled an assassination list. While these incidents appear largely episodic and suggest that, at least in 2015, ISIS had not yet developed a systematic reliance on Bitcoin for fundraising, they nonetheless demonstrate that NSAGs were beginning to recognize the potential utility of virtual currencies.

5. Conclusion and Policy Implications

We start with the observation that Web 3.0 technologies, most prominently decentralized applications, blockchain, and DeFi, function as a double-edged sword for governments and the general public. Importantly, inasmuch as Web 3.0 emphasizes user privacy and the individual control of data, NSAGs and other illicit groups may seek to take advantage of these novel applications to perpetrate terrorist attacks, commit human trafficking, drug trafficking, and other criminal activities. As a result, the absence of government supervision and crackdowns allows Web 3.0 technologies to potentially facilitate the operation of NSAGs on decentralized platforms. While this argument is intuitively compelling, there had yet to be a systematic exploration in political science literature that investigates how, and through which mechanisms, Web 3.0 applications influence the survival and operational strategies of NSAGs.

In this study, drawing upon insights from social movement theory, we develop a theoretical framework to understand how Web 3.0 technologies influence the organizational modes and structures of NSAGs. Specifically, we explore the mechanisms through which digital currencies, decentralized network applications, AI, and the Dark Web enhance key organizational functions of NSAGs, such as communication, recruitment, financing, and propaganda.

This study addresses a critical research gap at the intersection of Web 3.0 studies and political violence research by analyzing how NSAGs strategically exploit emerging digital technologies. Scholarship on Web 3.0 has largely emphasized its emancipatory potential, such as decentralization, personalization, and user empowerment, while overlooking its security implications. By documenting how NSAGs appropriate Web 3.0's core features, particularly anonymity, this study demonstrates that these same attributes enable illicit financing, recruitment, and operational resilience. In doing so, it expands mainstream understandings of Web 3.0 by highlighting the security implications it poses when appropriated by malign actors. At the same time, research on political violence has insufficiently engaged with technological transformations as drivers of organizational and strategic change among NSAGs. By foregrounding the role of Web 3.0, this study reveals how emerging digital technologies have functioned not merely as tools but as structural forces reshaping the dynamics of political violence. This positions technology not as an external variable but as a constitutive element of NSAG resilience and survival strategies. Taken together, the findings bridge a divide between technology studies and political violence scholarship. By focusing on the security implications of Web 3.0, this study aims to enrich our understanding of conflict in the era of Web 3.0, in which technological empowerment and unconventional security threats are deeply intertwined.

This research highlights that, in the Web 3.0 era, intelligence agencies and law enforcement face increasing challenges in tracking and disrupting the activities of NSAGs. Based on our theoretical analysis, two major policy implications reveal themselves.

First, nation-states should consider establishing international institutions to combat the transnational operations of NSAGs through Web 3.0 networks. As our analysis shows, the development of Web 3.0 technologies has significantly facilitated the expansion of NSAGs' digital networks, which can now easily transcend national borders. Notably, the financing channels of NSAGs are often tied to multiple financial institutions across different countries. Therefore, governments facing NSAG threats should collaborate to impose multinational sanctions on Web 3.0 financial services providers found to be facilitating NSAGs' cryptocurrency transactions. These sanctions could be complemented by implementing stricter regulations on cryptocurrency exchanges and, in some cases, limiting the anonymity features of privacy coins. Overall, international cooperation is essential to monitor and regulate DeFi platforms and smart contracts, which NSAGs may exploit for money laundering and financial transactions.

Second, government entities should also explore the potential of Web 3.0 technologies, leveraging these powerful decentralized applications to enhance their efforts against NSAGs. AI-powered threat detection models, in particular, present a promising tool. Given that NSAGs' operations on blockchains are typically anonymous and difficult to track using conventional methods, intelligence agencies and law enforcement can employ machine learning algorithms and AI to identify unusual patterns and trends in transnational financial transactions, communications, and other illicit activities. These AI-driven tools could enable governments to more effectively detect and disrupt NSAGs' clandestine operations. To this end, governments may consider allocating resources and providing policy support to research institutions focused on developing advanced technical tools to monitor NSAG activities on Web 3.0 networks, including their use of blockchain for encrypted communications, propaganda, and decentralized financial transactions.

Acknowledgments

The authors would like to thank the reviewers and editors for their valuable comments and feedback. They also extend their gratitude to Phillip Kraeter and David An for proofreading the article.

Funding

This study has received financial support from the National Social Science Fund of China (no. 25CGJ006).

Conflict of Interests

The authors declare no conflict of interests.

References

Abutaleb, Y., & Cooke, K. (2016, June 6). A teen's turn to radicalism and the U.S. safety net that failed to stop it. *Reuters*. https://www.reuters.com/investigates/special-report/usa-extremists-teen

Awasthi, S. (2024, May 8). Exploring the nexus: Cryptocurrency, Zakat, and terror funding. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/exploring-the-nexus-cryptocurrency-zakat-and-terror-funding

Baraniuk, C. (2017, July 21). AlphaBay and Hansa dark web markets shut down. *BBC*. https://www.bbc.com/news/technology-40670010

Barassi, V., & Treré, E. (2012). Does Web 3.0 come after Web 2.0? Deconstructing theoretical assumptions through practice. *New Media & Society*, *14*(8), 1269–1285.

Beck, C. J. (2008). The contribution of social movement theory to understanding terrorism. *Sociology Compass*, *2*(5), 1565–1581.

Berton, B. (2015). *The dark side of the web: ISIL's one-stop shop?* European Union Institute for Security Studies. https://www.iss.europa.eu/publications/alerts/dark-side-web-isils-one-stop-shop

Bharadiya, J. P. (2023). Artificial intelligence and the future of web 3.0: Opportunities and challenges ahead. *American Journal of Computer Science and Technology*, *6*(2), 91–96.

Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence*, *31*(6), 1242–1254.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Category deep-dive: Use of crypto in terrorist financing expanded in 2024. (2025, March 5). *TRM Labs*. https://www.trmlabs.com/resources/blog/category-deep-dive-use-of-crypto-in-terrorist-financing-expanded-in-2024

Coker, M., Schechner, S., & Flynn, A. (2015, November 16). How Islamic State teaches tech savvy to evade detection. *The Wall Street Journal*. https://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824

Copeland, T. (2021, May 12). Attacker uses flash loans in $24.5 million exploit of DeFi protocol xToken. *The Block*. https://www.theblock.co/post/104667/defi-protocol-xtoken-exploit-attack

Dilipraj, E. (2014). Terror in the Deep and Dark Web. *Air Power Journal*, *9*(3), 121–140.

Dodd, V. (2011, February 28). British Airways worker Rajib Karim convicted of terrorist plot. *The Guardian*. https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim

Englehart, N. A. (2016). Non-state armed groups as a threat to global security: What threat, whose security? *Journal of Global Security Studies*, *1*(2), 171–183.

Freeman, M., & Ruehsen, M. (2013). Terrorism financing methods: An overview. *Perspectives on Terrorism*, *7*(4), 5–26.

Ghatak, S., Gold, A., & Prins, B. C. (2019). Domestic terrorism in democratic states: Understanding and addressing minority grievances. *Journal of Conflict Resolution*, *63*(2), 439–467.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, Article 102498.

Huang, C. (2025, February 10). Illicit crypto volume drops in 2024, but use in terrorist financing up: Report. *The Straits Times*. https://www.straitstimes.com/business/illicit-crypto-volume-drops-in-2024-but-the-use-in-terrorist-financing-grew-report

Hyzen, A. (2023). Propaganda and the Web 3.0: Truth and ideology in the digital age. *Nordic Journal of Media Studies*, *5*(1), 49–67.

Jacksi, K. (2019). Design and implementation of e-campus ontology with a hybrid software engineering methodology. *Science Journal of University of Zakho*, *7*(3), 95–100.

Jacksi, K., Ibrahim, R. K., Zeebaree, S. R., Zebari, R. R., & Sadeeq, M. A. (2020). Clustering documents based on semantic similarity using HAC and K-mean algorithms. In *2020 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 205–210). IEEE.

Jacobson, M. (2010). Terrorist financing and the internet. *Studies in Conflict & Terrorism*, *33*(4), 353–363.

Jenkins, J. C. (1983). Resource mobilization theory and the study of social movements. *Annual Review of Sociology*, *9*(1), 527–553.

Johnson, G. (2022). *Will Web 3.0 secure a democratic future?* Tony Blair Institute for Global Change. https://institute.global/insights/tech-and-digitalisation/will-web-30-secure-democratic-future

Kurilovas, E., Kubilinskiene, S., & Dagiene, V. (2014). Web 3.0-based personalisation of learning objects in virtual learning environments. *Computers in Human Behavior*, *30*, 654–662.

Lassila, O., & Hendler, J. (2007). Embracing "Web 3.0." *IEEE Internet Computing*, *11*(3), 90–93.

LeVine, V. T. (1995). The logomachy of terrorism: On the political uses and abuses of definition. *Terrorism and Political Violence*, *7*(4), 45–59.

McAdam, D. (2017). Social movement theory and the prospects for climate change activism in the United States. *Annual Review of Political Science*, *20*(1), 189–208.

McLean, E. V., Hinkkainen, K. H., de la Calle, L., & Bapat, N. A. (2018). Economic sanctions and the dynamics of terrorist campaigns. *Conflict Management and Peace Science*, *35*(4), 378–401.

Meyer, D. S., & Staggenborg, S. (1996). Movements, countermovements, and the structure of political opportunity. *American Journal of Sociology*, *101*(6), 1628–1660.

Montieri, A., Ciuonzo, D., Aceto, G., & Pescape, A. (2018). Anonymity services Tor, I2P, JonDonym: Classifying in the Dark (Web). *IEEE Transactions on Dependable and Secure Computing*, *17*(3), 662–675.

Morris, A. (2000). Reflections on social movement theory: Criticisms and proposals. *Contemporary Sociology*, *29*(3), 445–454.

Murray, A., Kim, D., & Combs, J. (2023). The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons*, *66*(2), 191–202.

Nasar, M. (2023). Web 3.0: A review and its future. *International Journal of Computer Applications*, *185*(10), 41–46.

O'Brien, S. (2023, June 23). How Web3 security concerns might impact you. *IEEE Computer Society*. https://www.computer.org/publications/tech-news/trends/web3-security-concerns

Pearlman, W., & Cunningham, K. G. (2012). Nonstate actors, fragmentation, and conflict processes. *Journal of Conflict Resolution*, *56*(1), 3–15.

Podder, S. (2013). Non-state armed groups and stability: Reconsidering legitimacy and inclusion. *Contemporary Security Policy*, *34*(1), 16–39.

Prandini, M., & Ramilli, M. (2012). Raising risk awareness on the adoption of Web 2.0 technologies in decision making processes. *Future Internet*, *4*(3), 700–718.

Rapoport, D. C. (1983). Fear and trembling: Terrorism in three religious traditions. *American Political Science Review*, *78*(3), 658–677.

Rathor, S., Zhang, M., & Im, T. (2023). Web 3.0 and sustainability: Challenges and research opportunities. *Sustainability*, *15*(20), Article 15126.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, *16*(4), 482–494.

Rusumanov, V. (2016). The use of the internet by terrorist organizations. *Information & Security*, *34*(2), 137–150.

Ryan, N., Persi Paoli, G., Aldridge, J., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web*. RAND Corporation. https://policycommons.net/artifacts/4836375/behind-the-curtain/5673069

Sageman, M. (2011). *Leaderless jihad: Terror networks in the twenty-first century*. University of Pennsylvania Press.

Saravalle, E., & Rosenberg, E. (2018, January 9). Bitcoin can help terrorists secretly fund their deadly attacks. *Center for a New American Security*. https://www.cnas.org/publications/commentary/bitcoin-can-help-terrorists-secretly-fund-their-deadly-attacks

Shead, S. (2021, December 21). Elon Musk and Jack Dorsey are talking about 'Web3'—Here's what it is and why it matters. *CNBC*. https://www.cnbc.com/2021/12/21/elon-musk-and-jack-dorsey-are-talking-about-web3-heres-why.html

Shehabat, A., Mitew, T., & Alzoubi, Y. (2017). Encrypted jihad: Investigating the role of Telegram app in lone wolf attacks in the West. *Journal of Strategic Security*, *10*(3), 27–53.

Suh, D. (2001). How do political opportunities matter for social movements? Political opportunity, misframing, pseudosuccess, and pseudofailure. *The Sociological Quarterly*, *42*(3), 437–460.

Tekdal, M., Sayginger, Ş., & Baz, F. Ç. (2018). Developments of web technologies and their reflections to education: A comparative study. *Journal of Educational and Instructional Studies in the World*, *8*(1), 17–27.

TRM finds mounting evidence of crypto use by ISIS and its supporters in Asia. (2023, July 20). *TRM Labs*. https://www.trmlabs.com/resources/blog/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia

U.S. Department of Justice. (2017, July 20). *AlphaBay, the largest online 'dark market,' shut down* [Press release]. https://www.justice.gov/archives/opa/pr/alphabay-largest-online-dark-market-shut-down

U.S. Department of the Treasury. (2022, October 17). *Treasury designates al-Shabaab financial facilitators* [Press release]. https://home.treasury.gov/news/press-releases/jy1028

U.S. Department of the Treasury. (2024). *Supplemental advisory on the procurement of precursor chemicals and manufacturing equipment used for the synthesis of illicit fentanyl and other synthetic opioids* (FinCEN Advisory FIN-2024-A002). https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2024-a002

Vayadande, K., Baviskar, A., Avhad, J., Bahadkar, S., Bhalerao, P., & Chimkar, A. (2024, June). A comprehensive review on navigating the Web 3.0 landscape. In *2024 Second International Conference on Inventive Computing and Informatics (ICICI)* (pp. 456–463). IEEE.

Vittori, J. (2009). All struggles must end: The longevity of terrorist groups. *Contemporary Security Policy*, *30*(3), 444–466.

Wan, S., Lin, H., Gan, W., Chen, J., & Philip, S. Y. (2024). Web3: The next internet revolution. *IEEE Internet of Things Journal*, *11*(21), 34811–34825.

Wang, Y., Shen, Y., & Han, Z. (2022). Economic sanctions and state-sponsored terrorism: The case of Iran. *Israel Affairs*, *28*(5), 645–660.

Yuniar, R. W. (2017, January 10). Bitcoin, PayPal used to finance terrorism, Indonesian agency says. *The Wall Street Journal*. https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198

Zhang, X., Min, G., Li, T., Ma, Z., Cao, X., & Wang, S. (2023). AI and blockchain empowered metaverse for web 3.0: Vision, architecture, and future directions. *IEEE Communications Magazine*, *61*(8), 60–66.

Zhu, J., Li, F., & Chen, J. (2024). A survey of blockchain, artificial intelligence, and edge computing for Web 3.0. *Computer Science Review*, *54*, Article 100667.

Zuo, Z. (2023). Development, application, and regulation of Web3.0. *Frontiers in Business, Economics and Management*, *9*(3), 22–27.

About the Authors

Yaohui Wang is a lecturer at Zhou Enlai School of Government, Nankai University. He has published before in *Politics and Governance*, *Journal of Contemporary China*, *Climatic Change*, and other journals.

Yang Qiu is a PhD candidate at Zhou Enlai School of Government, Nankai University. His research interests include transatlantic relations and security policy.