NATIONAL INTELLIGENCE COUNCIL

MEMORANDUM

NIO PERSPECTIVE

5 July 2023

Non-State Actors Playing Greater Roles in Governance and International Affairs

Key Takeaways

Scope Note: *This paper provides a baseline assessment of the role of non-state actors in international and national security affairs. It was self-generated by the National Intelligence Council to inform a review of the IC's work related to non-state actors, as both topics of study and partners. We broadly define non-state actors to include both nongovernmental and subnational governmental entities.*

Since the end of the Cold War, non-state actors (NSAs) have had an increasing and more consequential role in global dynamics—a trend that is likely to continue even as globalization slows. A more divided and contested global landscape, less adaptable state institutions, and greater capability and resourcing available outside governments are giving NSAs greater influence in and across multiple global domains.

- NSAs comprise a broad variety of entities, including subnational governments, commercial firms, academic and scientific institutes, civil society movements, militants and other criminal groups, and even super-empowered individuals. Each type of entity brings unique capabilities and varying degrees of influence to bear on the goals of and dynamics within and between states.
- The influence and impact of NSAs vary from providing societal services, intelligence, security, paramilitary capabilities, and governance that at times place them in direct competition with state institutions, to addressing transnational challenges and in so doing, helping to shape norms, values, and standards that give them prominence apart from states.
- This increasing capability and influence of NSAs in international and national affairs—particularly those involved with key technologies or critical infrastructure—also have made them a more direct target of states looking for a strategic advantage, making their protection from such threats another key factor in the global order and great power competition.

Increasing Influence

The declining adaptability of state institutions, a more divided and contested international environment, and the increasing availability of both resources and new capabilities outside government are making non-state actors (NSAs) more important and relevant to the goals of sovereign national governments, and stronger competitors in areas that nation-states have tended to dominate. The growing role of NSAs in global dynamics and national security affairs has been a focus of the IC for several decades.

- State-controlled institutions in every region and every government type are facing greater challenges meeting the expectations of their populations, according to think tank analysis, a particularly strong trend in weak or failed states. Publics globally now trust businesses and NGOs more than governments, according to survey research by a global communications firm. Additional studies show a corresponding rise in social unrest globally, with the number of protests increasing since 2012 and the number of organized protest movements tripling between 2006 and 2020. The majority of these events have been prompted by the perceived failure of political systems or representation.

- At the same time, many of the multilateral institutions that have served as the core pillars of the international system are struggling to respond to emerging challenges and meet public demands. Some, such as the WHO and other international development organizations, have longstanding weaknesses and divisions that were exposed and exacerbated by the COVID-19 pandemic, according to open-source reporting, raising questions about international willingness and ability to cooperate on common challenges. Others, such as UN security institutions and the WTO, face growing political deadlock that will limit their ability to address contentious issues.

- Intensifying US strategic competition with China and Russia has strained nation-state cooperation regionally and internationally on areas of global concern, including through nation-state collectives. As differences among the Permanent Five (P5) UNSC members have become sharper since 2012, China has increased its veto rate in the UNSC, casting 12 vetoes since 2010 after only three from 2000 to 2010, according to UN data. We assess that the mere threat of Beijing's veto compounds UNSC gridlock on global security issues.

Concurrently, NSAs, which have long provided governance services in all state types, are positioned to take up more of the slack within countries and internationally, and already are an integral part of US policy efforts in areas such as building state resilience, health care, and climate response, particularly in the developing world.

- We assess that technological advances are further empowering NSAs globally by improving their provision and distribution of services, enabling them to attract funding and other resources, and facilitating their collaboration with each other and others. Communication and collaboration tools are improving the ability of NSAs to network among groups, engage directly with populations, and broaden their reach across both national borders and transnational issues. Other scientific and technological advances, such as AI, additive manufacturing, and biotechnology are at the threshold of enabling these actors to even more rapidly deliver tailored solutions to at-need groups, according to open-source and trade publications. At the same time, these technological advances make it easier for violent NSAs to conduct more and more lethal operations, according to the analysis of several prominent institutions.

- We assess that many NSAs have other inherent advantages that enhance their operational agility and resulting influence, including their focus on and specialization in particular issues. Those with on-the-ground access and existing networks can more easily adapt to local dynamics, engender trust, and leverage this to press state and multinational organizations to take action, according to open-source and academic information. Press and academic reporting suggest some will press the boundaries of and even overstep regulatory frameworks, particularly where governmental organizations have weak representation or authority.

- Recognizing these advantages, state leaders and institutions also increasingly look to partner with NSAs in pursuit of national and international policy goals, according to one prominent research organization. For example, partnerships with service organizations and civil society groups are an explicit part of both the US

Strategy to Prevent Conflict and Promote Stability from 2020 and its *Strategy to Anticipate, Prevent, and Respond to Atrocities* from 2022, according to open-source and US State Department information. Iran also utilizes NSAs to pursue regional agendas, for example, cooperating with Iraqi Shia militant groups such as Asa'ib Ahl al-Haq and Kata'ib Hizballah to counter the US presence in Iraq, according to open-source reporting.

More Entities With Expanding Abilities

We assess NSAs also are becoming more capable, generating a greater diversity of effects and influence in international and national security affairs. Although they lack the privileges and rights of politically sovereign actors, these entities exercise significant economic, political, or social power at a national and even international level. While NSAs with such influence traditionally have functioned as distinct actors with a clear organizational structure, increasingly more diffuse collectives and even individuals lacking a distinct hierarchy or formal operational network are wielding influence at larger scales, and in more variable ways. For the purpose of this study, we have chosen to group these entities into seven architypes based on primary function or motive, none of which are mutually exclusive.

- **Governments below national level**—whether regional, provincial, or local—are founded and operate around the delivery of services in exchange for some level of sovereign authority. Some of these governments—in the United States and elsewhere—are formulating their own subnational foreign policies, pursuing outreach and cooperative partnerships with other sovereign national and subnational governments.

- **Commercial entities** provide services or capabilities for profit or to support profit generating enterprises and often are at the forefront of technological and other types of innovation. They include multinational corporations; media organizations and social media platforms; lobbyists; subject matter experts; and private banking, investment, and credit-rating institutions.

- **Academic and research institutions** provide education, create and distribute new knowledge through their research efforts, bring scholars together to work on shared subjects, and influence the socializing of ideas, principles, and norms through classroom and professional networks and publications.

- **Public service organizations** typically exist to provide public services on a not-for-profit basis or to promote or otherwise support other organizations offering such services. These can include foundations, charities, philanthropic organizations, or organizations that advocate for particular special interests within a society.

- **Civil society entities** include a wide set of actors that range from political parties, trade unions, and professional organizations to tribal structures, religious groups, and protest movements, with a common purpose of helping to unite and support the needs of a particular sector of a community.

- **Illegal and extra-legal organizations** are driven by profit, ideology, or some combination of both, intentionally operating outside the legal and normative structures within a society. They include organized criminal enterprises such as illicit drug cartels and human smuggling rings, violent extremist or terrorist organizations, paramilitary organizations, disinformation for-hire firms, and cyber criminals, but also can include entities looking to exploit areas for which few or no legal or regulatory frameworks have yet been established, such as companies seeking to trade in cryptocurrencies or carbon futures.

- **Super-empowered individuals**—a growing form of NSAs—include celebrities, business moguls, social media influencers, and hackers who capitalize on their popularity, wealth, or talents to draw attention to issues, mobilize

societies, and even marshal resources to address particular causes. Companies and high-profile public figures are acquiring sufficient economic power and international reach to influence both social and geopolitical issues worldwide, according to open sources.

Widespread Engagement and Geopolitical Influence

NSAs are engaging in a variety of activities that complement, compete with, and sometimes bypass the goals and activities of national-level governments and multinational bodies that form the traditional foundation of the international system. They often will operate across multiple areas, which we assess further boosts their reach and influence. Examples of the variety of specific NSAs and their activities include:

Providing Societal Services and Governance.

- The French-founded **Medecins Sans Frontieres (Doctors Without Borders)** operates in more than 70 countries, employs more than 45,000 people, and has a reported annual income of almost $2 billion, according to the organization's own reports and other open-source information.

- **Social media platforms**—including foreign applications such as China's **QZone**, Russia's **VKontakte**, and France's **BeReal**—have become powerful means for personal communications previously handled by postal and telecommunications services and mass advertising previously dominated by print media.

- The **International Telecommunications Union (ITU)** and **3GPP** are international standards setting entities comprised of industry organizations whose members participate voluntarily to establish common practices that promote interoperability.

- **The global open-source software community** creates software applications and components comprising roughly 75 percent of the code used by global software companies in support of 17 sectors including energy, health care, aerospace, and technology, according to an industry survey from 2020 that evaluated supply chain risks. Although these programmers have developed large quantities of important open-source code, they have introduced programming error —sometimes deliberately—causing outsized disruptions that spanned diverse industries, or sparked widespread hacking and ransomware campaigns by state and non-state actors.

Offering Intelligence, Security, and Paramilitary Capabilities.

- The Netherlands-based **Bellingcat** is a self-described independent investigative "collective" comprised of about 18 professional staff and a network of volunteers who use open-source information—including commercial imagery and telephone metadata—to conduct investigations of topics that, at one time, only state-run security and law enforcement organizations had the resources to perform. Its founder has described the group as "an intelligence agency for the people."

- **Team Jorge** is an Israel-based company that offers intelligence, cyber, and influence services. Its staff consists of former intelligence and special forces officers and media experts from Israel, Russia, Spain, the United Kingdom, and the United States. In 2022, it alleged to have influenced 27 out of 33 different presidential campaigns it was targeting, in part, using its proprietary Advanced Impact Media Solutions product to create virtual profiles, and circulate and propagate disinformation on a mass scale and in any language.

- **Vagner** is a Russian private military and security company that provides mercenary services in countries across Africa and the Middle East, and until July, alongside Russian forces in Ukraine, according to open sources, and had been closely associated with both directly and indirectly assisting Moscow's foreign policy goals. It recently mounted an ultimately aborted internal armed rebellion aimed at overturning the military leadership of Russia.

Addressing Transnational Challenges and Protecting Global Common Areas.

- **Greenpeace** is a nongovernmental organization that promotes environmental causes, sometimes via controversial means, and according to its website, is reliant on funding from foundational grants and individual supporters. Reportedly, the Russia branch is being forced to close because the state Prosecutor General's office declared that its activities are a threat to the fundamental constitutional order and security of the Russian Federation, according to press reporting.

- The **Tony Blair Institute for Global Challenges** emphasizes the constructive use of technology in helping leaders develop and implement policies in areas such as expanding Internet access in Africa and strengthening public health institutions, according to its website. The Institute also has convened a Global Health Security Consortium with the goal of transforming global health infrastructure to better address preventable disease.

Shaping Norms, Values, and Behavioral Standards.

- A **US startup firm** announced it conducted an unregulated geoengineering experiment in Mexico last year and another experiment in the southwestern United States in February, apparently seeking to draw attention to the lack of progress toward climate mitigation and promote greater acceptance of commercial geoengineering ventures. Researchers with the UK-based **European Astrotech** launched a similar experiment last fall, according to an academic publication.

- **Intellexa** is an alliance of for-profit hacking firms operating out of Europe and Asia that have been able to attract and retain business from nations no longer able to buy Israeli hacking tools to target political opponents, journalists, and civil society organizations because of new Israeli Government restrictions, according to open-source information. The Israel-based surveillance software company **NSO Group** has provided its services to multiple countries, allegedly including five EU member states, and its software has been used to target political opponents, journalists, and civil society organizations, according to open-source information.

- The Russia-based **Internet Research Agency** conducts large-scale propaganda disinformation campaigns to manipulate international public opinion, sow fear, and erode trust in political and media institutions to the benefit of foreign governments or businesses, according to open-source reporting. Similarly, **Africa Politology**—Vagner owner Yevgeniy Prigozhin's political strategy organization—supports Russia-friendly politicians, undermines Western influence, and discredits the UN.

- **Anonymous** is a decentralized collective of international hacktivists who promote leftist-libertarian ideals of personal freedom and oppose the consolidation of corporate and government power, according to press reports. For example, hackers claiming to be affiliated with Anonymous recently threatened the Pakistani Government over crackdowns on protests following the arrest of former Prime Minister Imran Khan. However, its lack of centralized organization or control sometimes results in hackers acting under the Anonymous banner but undertaking cyber attacks in support of contradictory goals.

Threatening Lives and Livelihoods.

- **ISIS** has suffered major setbacks since the apogee of its power in 2014, but its affiliates and those of **al-Qa'ida** maintain the intent to attack targets internationally, according to counterterrorism experts. The threat from **racially or ethnically motivated violent extremist movements** also has been on the rise internationally.

- The **Sinaloa Cartel** and the **Cartel Jalisco Nueva Generacion (CJNG)**—the two dominant Mexico-based **transnational criminal organizations (TCOs)**—are responsible for trafficking illicit fentanyl to the United States that led to more than 109,000 American overdose deaths last year. Mexican TCOs and affiliated human smuggling organizations are exploiting and profiting from US-bound irregular migrants transiting Mexico by charging smuggling fees and kidnapping migrants for ransom, and some become victims of forced labor and sex trafficking in Mexico and the United States, according to press.

- **Cyber criminal groups** such as China's **APT41** have a mix of private and government ties, according to open-source reporting, blurring the distinction between state activity and traditional cybercrime.

Implications for the United States

We assess that the factors driving the increased prominence of NSAs in international and national security affairs will persist, further enabling even greater NSA capacity and influence and increasing both their utility to states as partners and their capacity to challenge or complicate nation-state policy goals. However, we also assess that they are unlikely to collectively eclipse the power of the state-centric international order in the foreseeable future because their influence—and power derived from it—tends to be concentrated in narrow areas. Intensifying competition among nation-states makes it unlikely, moreover, that sovereign governments will yield too much agency and control to others, including to and over NSAs, and particularly within their borders. The operations of NSAs still are significantly affected by local, national, or international systems dominated by sovereign state authorities that regulate—and to varying degrees monitor—their activities.

- The specialized subject matter expertise or access to particular geographic areas or communities that NSAs can bring to bear can augment US, allied, and partner state capabilities, as they can for adversaries. Examples could include relying on a nongovernmental organization to provide translators for certain language dialects or access to remote locations, or working with an armed NSA to provide security in areas where sending a persistent US or other nation-state military presence is not desired.

- NSAs that originate in the developed world and work within the framework provided by Western institutions and regimes can promote "western values" such as free markets, environmental protection, and human rights. However, those originating in and beholden to China and other authoritarian regimes can do the same for their respective governments

- NSAs also potentially can serve as honest brokers in areas in which state governments are seen as too politically driven, both on shared and contested interests.

However, NSAs still have their own goals and agendas that can diverge from US and other nation-states' policy interests, and many are likely to seek to influence as well as inform the policy decisions of the state officials and institutions they work with. Depending on the actor and the situation, techniques could include persuasion, framing issues in a way that brings public or private pressure to bear, bribery, and potentially even violence.

- NSAs can form agreements with other governments or entities that might not align with Western values or US policies, and even act to influence foreign policies in allied and partner nations. Others may be unwilling to cooperate out of concern that aligning with the United States would negatively affect their operations. The same challenges will affect NSAs critical of or at least not wanting to appear sympathetic to US adversaries and authoritarian regimes.

- NSAs also can facilitate or instigate societal actions or trends that are disruptive for governments and challenge local, national, or international norms of behavior. For example, they can use social media platforms to promote undesirable behaviors and urge disruptive—even violent—actions. Weak, conflicting, or nonexistent national and international standards for governing emerging and rapidly developing technological capabilities, such as AI and biotechnology, also are likely to give NSAs wide latitude to navigate the space, and influencing the norms and rules for governing these technologies.

This increasing capability and influence of NSAs in international and national security affairs—particularly those involved with key technologies or critical infrastructure—also have made them a more direct target of states looking for a strategic nation-state advantage, making their strength and protection from threats another key factor in the global order and great power competition. China, for example, has stolen hundreds of gigabytes in intellectual property from multinational companies in Asia, Europe, and North America in an effort to leap-frog over technological hurdles, according to open-source reporting, with as much as 80 percent of US economic espionage cases as of 2021 involving PRC entities.