BIPSS Commentary
www.bipss.org.bd
July-2024
BIPSS
Towards a Secure World

The Strategic Use of AI by Non-State Actors: Implications for Global Security

Mohosina Mostofa[1]

Source: LimkedIn

Introduction

In today's world, artificial intelligence (AI) is everywhere. It helps us with daily tasks, from voice assistants on our phones to smart algorithms that suggest what to watch next. But while many people think of AI as a tool for convenience, it is also being used in unexpected ways, especially by non-state actors like terrorist groups, criminal organizations, and hacktivists. These groups are using AI strategically to carry out their plans, whether that is spreading propaganda, hacking into systems, or even planning attacks. This shift raises serious questions about global security. As these

[1] Mohosina Mostofa is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the Bangladesh University of Professionals (BUP).

non-state actors gain access to powerful AI tools, the landscape of conflict and safety is changing dramatically.

In this commentary, it will be explored how non-state actors use AI, what this means for global security, and why we need to pay attention to this emerging threat. Understanding these implications is crucial, as they can shape the future of peace and safety around the world.

The Influence of Non-State Actors on Global Security

Non-state actors are groups that operate independently from government authority. Unlike traditional armies or government organizations, these actors include a wide range of entities such as terrorist organizations, criminal syndicates, and activist groups.[2] Their influence on global security is significant and complex.

One key aspect of non-state actors is their ability to operate across borders, transcending the limitations of national governments. This allows them to engage in various activities, from promoting social causes to conducting illicit operations. Their transnational nature means that they can respond quickly to global issues, sometimes filling gaps left by states or international organizations. Moreover, non-state actors often leverage technology and social media to amplify their influence.[3] They can mobilize support, spread information, and raise awareness about specific issues more effectively than traditional entities. This digital presence enables them to connect with a wider audience, making their messages resonate in diverse communities.

The motivations of non-state actors can vary greatly. While some pursue altruistic goals, such as humanitarian assistance or environmental protection, others may aim to disrupt social order or challenge existing power structures. This diversity complicates the security landscape, as governments and international bodies must address both positive and negative contributions from these actors. Besides, the rise of non-state actors has implications for state sovereignty. As these entities gain power and influence, they can undermine the authority of nation-states, challenging

[2] “Transnational Organized Crime: A Growing Threat to National and International Security”, National Security Council, https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat

[3]“Balancing and Adopting to The Rise of Non-State Actors!”, Press Xpress, May 27, 2024, https://pressxpress.org/2024/05/27/balancing-and-adapting-to-the-rise-of-non-state-actors/

their ability to maintain order and security. This shift requires a reevaluation of security strategies, as traditional approaches may not effectively address the complexities posed by non-state actors.

The Strategic Use of Artificial Intelligence by Non-State Actors

Creation of Autonomous Weapons

Non-state actors are increasingly exploring the development of autonomous weapons systems powered by AI. These systems can identify and engage targets without direct human control. This capability makes them appealing for asymmetric warfare, where smaller groups can leverage technology to match state capabilities.[4] Autonomous weapons can operate drones or ground vehicles that make real-time decisions based on their environments. For instance, they can analyze data from sensors to determine threats and launch attacks autonomously. This level of automation reduces the need for human operators, potentially lowering the risk of casualties for the attacking group. However, it raises significant ethical concerns about accountability and the potential for misuse.

Source: Air University

[4] Stuart Russell, "Why we need to regulate non-state use of arms", Forum Institutional, May 18, 2022, https://www.weforum.org/agenda/2022/05/regulate-non-state-use-arms/

Enhanced Cyber Attacks

Non-state actors, such as hacker collectives and cybercriminals, are using AI to execute more sophisticated cyber-attacks. AI technologies enable them to automate hacking processes and improve their success rates. AI can be utilized to develop tools that perform automated phishing attacks, where malicious actors send fraudulent messages to trick individuals into revealing sensitive information.[5] AI algorithms can analyze vast amounts of data to identify weaknesses in security systems, allowing attackers to bypass traditional defenses. This makes it difficult for organizations to keep up with the rapidly evolving tactics employed by these groups.

Source: E-international Relations

Disinformation and Deepfakes

Non-state actors are leveraging AI to create convincing deepfake content—manipulated audio, images, or videos that appear authentic. This technology can be used to spread disinformation, manipulate public opinion, or undermine trust in institutions. For example, AI-generated deepfake videos can depict public figures saying or doing things they never actually did, causing confusion and inciting unrest. This manipulation can lead to significant social discord, affecting political stability and public trust. The ability to produce and distribute such content quickly enhances the capacity of these actors to influence narratives and create chaos.

[55]Stuart Russell, “Why we need to regulate non-state use of arms”, Forum Institutional.

Financial Crimes

AI is being employed by non-state actors to facilitate various financial crimes, including identity theft, credit card fraud, and money laundering. By analyzing large datasets, these actors can identify vulnerabilities and potential victims. Advanced algorithms can sift through public and private data to pinpoint individuals likely to fall victim to fraud. Criminal organizations may use AI to automate the process of creating fake identities or laundering money through complex transactions that evade detection. This ability to analyze and act upon data rapidly increases the scale and efficiency of their operations.

Surveillance and Information Gathering

Non-state actors are increasingly using AI-driven surveillance techniques to monitor individuals, companies, and even governments. These methods allow them to gather critical information for planning operations or manipulating targets. AI algorithms can analyze data from various sources, including social media and public records, to uncover sensitive information. This data mining can reveal personal details, organizational structures, or weaknesses in security protocols. With this information, non-state actors can execute more strategic and targeted actions, whether for recruitment or operational planning.

Radicalization and Recruitment

AI technologies are being harnessed to identify individuals vulnerable to radicalization and tailor online content to influence their views. This capability aids non-state actors in recruiting new members. This technology has been used by terrorist groups like Hitzb-ut-Tahrir and other influential groups.[6] By analyzing online behavior and preferences, AI can determine which individuals might be susceptible to extremist ideologies. Non-state actors can then use this data to create targeted propaganda that resonates with these individuals, increasing the likelihood of recruitment. This process poses a significant challenge for counter-radicalization efforts, as it allows extremist groups to reach potential recruits effectively.

Creating Diversions and Confusion

[6] ibid

Non-state actors can use AI-generated distractions to mislead security forces and the public during operations. This tactic can create confusion, allowing them to execute their objectives more effectively. For example, AI could be employed to generate fake social media posts or alerts that draw attention away from a real attack. This diversion strategy can lead to a breakdown in communication among security forces, making it easier for the non-state actors to carry out their plans without detection. The ability to manipulate information flow enhances the chaos during critical situations.

Evasion of Cybersecurity Measures

AI is being utilized by non-state actors to circumvent traditional cybersecurity mechanisms, making it increasingly difficult for organizations to protect themselves against attacks. By employing machine learning algorithms, these actors can develop methods to bypass firewalls, intrusion detection systems, and other security measures. This adaptability allows them to launch attacks that can evolve in response to the defenses they encounter. The sophistication of AI-driven cyber-attacks necessitates continuous updates and improvements in cybersecurity technologies.

Case Study: The Extremist Groups' Propaganda Efforts

Source: Security Web Portal

Earlier in July 2024, Spanish authorities arrested nine young individuals who were spreading propaganda supporting the Islamic State (IS) group.[7] Among them was a man who specialized in creating multimedia content using AI editing tools. According to Moustafa Ayad from the Institute for Strategic Dialogue (ISD), AI enhances the propaganda efforts of groups like IS and al-Qaeda, allowing supporters to produce emotional content that rallies their base around core ideas.[8] This type of material is often crafted to avoid detection by content moderators on social media platforms, making it more likely to be shared among followers. In the past, IS has even used AI to produce amusing yet disturbing content, like videos featuring US presidents singing their war songs, showcasing their early adoption of new technologies for propaganda purposes.[9] While some of this content may appear trivial, it can still foster a sense of community and commitment among supporters.

Experts highlight the potential dangers of AI in the hands of extremist groups. Beyond propaganda, there are concerns that such groups could use AI chatbots to engage with potential recruits, paving the way for human recruiters to take over the conversation. Although AI models have built-in restrictions to prevent harmful use, these safeguards can sometimes be bypassed. There is also fear that extremists could leverage AI for digital attacks or to plan real-life terror operations. Despite these worries, analysts argue that the immediate threat still lies in the actual physical attacks these groups carry out. Research has shown that there isn't a direct correlation between the amount of propaganda produced by IS and their actual attacks. While the use of AI by these organizations is troubling, the real danger remains their ability to inspire attacks and recruit members, especially as they exploit current geopolitical tensions, like the recent conflict in Gaza, to further their agenda.

Challenges to Global Security

Diminished Predictability of Threats

The ability of non-state actors to utilize AI for autonomous decision-making can lead to unpredictable actions that are difficult for security agencies to anticipate. Unlike traditional methods, AI-driven strategies can evolve rapidly, enabling these actors to launch attacks or

[7] Cathrin Schaer, "How extremist groups like 'Islamic State' are using AI", July 10, 2024, https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398

[8] Cathrin Schaer, "How extremist groups like 'Islamic State' are using AI"

[9] ibid

propaganda campaigns without warning. This unpredictability complicates intelligence gathering and threat assessment, making it harder for governments to respond effectively.

Increased Information Warfare

AI tools allow non-state actors to flood information channels with disinformation, deepfakes, and misleading narratives. This capability can erode trust in legitimate news sources and create social division.[10] As societies grapple with misinformation, it becomes more challenging for governments to maintain stability and public trust, which can lead to unrest and conflicts that further jeopardize global security.

Rapid Proliferation of Advanced Technology

Non-state actors can leverage AI to quickly develop and deploy advanced technologies, including autonomous drones and sophisticated hacking tools, without the same regulatory oversight as nation-states.[11] This rapid proliferation can create a landscape where dangerous technologies are accessible to smaller groups or individuals, increasing the potential for large-scale attacks or disruptive acts that strain global security systems.

Erosion of Accountability

The use of AI by non-state actors blurs the lines of accountability, especially in instances involving autonomous weapons or cyber-attacks. It becomes difficult to attribute actions to specific individuals or groups, complicating the international community's ability to hold perpetrators accountable. This lack of accountability can embolden non-state actors, leading to an increase in aggressive actions without fear of repercussions.

Challenges to Law Enforcement and Regulation

The sophistication of AI applications used by non-state actors poses significant challenges for law enforcement agencies. Traditional methods of policing and regulation may become inadequate in addressing the rapidly changing tactics and technologies used by these groups. As a result, law

[10] Tatya Verma, "AI in Cyber Warfare", April 1, 2024, https://tdhj.org/blog/post/ai-cyber-warfare/

[11] "Adressing Risks from Non-State Actors' Use of COTS Tech", 2023, https://www.dhs.gov/sites/default/files/2023-09/07.%20Addressing%20Risks%20of%20COTS%20Tech_508_0.pdf

enforcement may struggle to keep pace with criminal innovations, leading to an increase in successful attacks and criminal activities that threaten public safety and security on a global scale.

Conclusion

AI is transforming our world in ways that are both exciting and concerning. On one hand, it offers incredible opportunities for progress and innovation, but on the other, it can be a powerful tool in the wrong hands. As non-state actors increasingly use AI to enhance their operations—whether through complex cyberattacks, spreading disinformation, or other malicious activities—we are confronted with challenges that demand swift and collective action. In response, it is essential for governments, tech companies, and civil society to unite in developing comprehensive frameworks that govern the ethical use of AI, strengthen security, and ensure transparency. This requires a global effort, with countries and organizations working together to share knowledge, establish best practices, and anticipate potential threats.

But beyond just reacting to these challenges, we need to be proactive. By fostering international cooperation and encouraging innovation in AI security, we can outpace those who seek to misuse this technology. The stakes are high—not just for our safety, but for the future of our interconnected world. Our collective ability to navigate this new landscape will determine whether AI becomes a force for progress or a tool for division. It's up to all of us to ensure that AI contributes to a safer, more stable, and prosperous world.