“

The weaponisation of drones shows how cyberspace functions as both facilitator and force multiplier: it can connect intent with capability, and radicalisation with precise technical guidance

How open knowledge in cyberspace fuels drone weaponization

by **Lara Maria Guedes Gonçalves Costa**

Weaponizing drones in the digital age

In a widely reported case, a teenager in the United States (US) posted a YouTube video of a home-made drone firing a handgun and later modifying it with a functional flamethrower to roast a turkey. The video allegedly received backing from "HobbyKing," an online drone parts retailer, while the flamethrower's fuel pump came from Amazon.[1]

After allegations that he threatened to shoot people, he was expelled from a university. This incident illustrates the reality of improvised weapons production, driven by open knowledge and the diffusion of the dual-use technology know-how in cyberspace.

Improvised weapons are not new. The use of improvised explosive devices (IEDs) and small arms and light weapons (SALW) in both conflict and non-conflict settings is well documented.[2] However, uncrewed aerial vehicles (UAVs, or drones) have recently drawn renewed attention. In the ongoing war in Ukraine, civilians have adapted hobby drones into low-cost loitering munitions and reconnaissance tools.[3] In Central America, modified drones have been used for smuggling, surveillance, and attacks.[4] These examples reflect a surge in do-it-yourself (DIY) drone weaponization, a phenomenon amplified by the digital domain.

1 Ben Popper, "The Teenager Behind the Drone Gun Now Has a Drone-Mounted Flamethrower", The Verge, 8 December 2015.

2 See, for example: Matilde Vecchioni, "Unregulated Production: Examining Craft-Produced Weapons from a Global Perspective", UNIDIR, 20 June 2024.

3 Isabel Coles and Ievgeniia Sivorka, "Four Ways Ukraine's Drone Innovations Are Changing Warfare", The Wall Street Journal, 12 October 2024.

4 Henry Ziemer, "Illicit Innovation: Latin America Is Not Prepared to Fight Criminal Drones,", Center for Strategic and International Studies, 11 June 2025.

Guidance is only a click away. Online tutorials and open-source designs have been shaping perceptions and influencing youth in cyberspace, who are both prominent users of digital spaces and key figures in drone maker communities. As this trend grows, understanding these dynamics is critical to addressing the normalization of violence and the misuse of emerging technologies.

Open-source knowledge and the DIY community

UAVs are no longer prohibitively expensive and limited to a few states.

> **"The global market for commercial UAVs is forecast to grow from US$7.2 billion in 2022 to US$19.8 billion by 2031.[5]"**

In parallel, technological simplification has lowered the expertise required to operate or modify drones.[6] This accessibility has attracted not only armed groups and criminal networks, but also lone actors eager to explore and execute plots with information found online.

Instructions on building or modifying drones are readily available across digital communities. "DIY Drones," the world's largest group of drone enthusiasts, counts over 80,000 members worldwide.[7] While many such networks promote responsible innovation, their open and unregulated nature makes oversight difficult. Contrary to the belief that weaponization content is confined to the Dark Web, tutorials on mainstream platforms like YouTube demonstrate how to attach payloads, including weapon systems, to consumer drones.

---

5 "Teal Group Predicts Worldwide Civil UAS Spending of $139 Billion Over the Next Decade in Its 2022/2023 UAV Market Profile and Forecast-Teal Group", Teal Group Corporation, 4 November 2022.

6 Gregory D. Koblentz, "Emerging Technologies and the Future of CBRN Terrorism", The Washington Quarterly 43, no. 2, 2 April 2020: pp. 185–86.

7 DIY Drones: The Leading Community for Personal UAVs, last accessed 2 August 2025.

Entertainment-oriented channels have also entered the space. Series of videos like "Game of Drones" showcase a team arming drones with flamethrowers, rockets, and paintball guns with live targeting systems.[8] Most creators claim these projects are non-commercial and experimental, yet they still represent improvised weaponization. Viewer comments, often from young people, praise these designs and express interest in replicating them. The unregulated sharing of such modifications online makes it easy to repurpose them for harm.

The cultural imaginary of drones and violence

To understand this phenomenon's impact on youth, it is crucial to look beyond the existence of DIY drone tutorials and examine why they attract so many viewers, particularly young people. The reasons youth might engage in crime or terrorist activity vary, but one often-overlooked driver is the growing culture of militarization performed and promoted through the digital domain.

Scholars have long noted how different media sources shape the way people see, think about, and justify violence.[9] While depictions of violence in entertainment are not a novelty (e.g., in movies), the weaponization of drones has introduced new ways of imagining and normalizing it. In popular video games such as "Battlefield" and "Call of Duty," drones are designed to match real-world specifications and operate as lethal tools in virtual combat.[10] App stores host games featuring lethal UAVs, including ones where players hunt people.[11] These games also feature narratives, such as depictions of how a US-China drone war would look in 2025.[12] Often presented without reflection or criticism, such entertainment frames UAVs as ordinary consumer products rather than tools of violence.

[8] Marque Cornblatt Productions, "Paintball Drone Gunship - a DIY Combat UAV from Game of Drones", YouTube, 10 June 2013
[9] See Vieira and Krcmar (2011), Dillio (2014), Dholakia and Reyes (2018).
[10] Roger Stahl, "What the Drone Saw: The Cultural Optics of the Unmanned War", Australian Journal of International Affairs
[11] Stahl, "What the Drone Saw," pp: 667-668.
[12] *Ibid.*, p. 666.

It is crucial to note that the interest of the DIY community in weaponizing drones is part of a "wider cultural imaginary,"[13] a shared set of ideas and expectations in society about what drones are for. Beyond fictional scenarios in video games, these imaginaries are also shaped by real-world state practices.[14] People are generally aware of the historical use of drones by the military (e.g., US lethal UAVs in counterterrorism), especially given freely accessible footage online. Police forces have also explored the idea of deploying drones for civil unrest, for example through the use of pepper spray-equipped UAVs.[15]

> **"Even when intended for non-lethal or controlled use, the operational deployment of UAVs by state authorities feeds into a cultural narrative that travels – people see it, absorb it, and replicate it."**

This influence is visible in the rise of "DIY warfare," rooted in the "maker culture" that values informal, peer-led learning.[16] In Ukraine, for example, soldiers have worked alongside young civilians to build drones and counter-UAV solutions.[17] This knowledge-sharing has crossed into the open, unregulated online space. Today, online videos show how to build "kamikaze drones," UAVs designed to self-destruct upon reaching a target.[18] One widely viewed online tutorial, produced by a former combatant with over one million YouTube subscribers,[19] has been widely praised by drone enthusiasts, including youth, turning state-sanctioned violence into part of everyday entertainment and hobbyist culture.

Moving youth away from harmful content

The weaponization of drones shows how cyberspace functions as both facilitator and force multiplier: it can connect intent with capability, and radicalization with precise technical guidance. This creates a growing transnational threat that bypasses traditional arms regulation. Addressing it requires a multi-stakeholder approach.

While online content moderation raises debates about free speech and privacy,[20] "freedom from fear" must also guide these discussions. This means recognising that regulating harmful content is as essential as protecting legitimate expression. The Global Internet Forum to Counter Terrorism (GIFCT), founded by major tech companies,[21] should continue and strengthen its work to reinforce platform accountability, including through the development of more robust moderation and reporting tools to address weaponization-related content, while safeguarding lawful innovation.

Governments should ensure that cyberspace governance discussions include the risks posed by open-source knowledge related to emerging technologies. This requires engaging a broad range of

[13] Anna Jackman, "Consumer Drone Evolutions: Trends, Spaces, Temporalities, Threats", Defense & Security Analysis 35, no. 4, 24 October 2019: p. 370.

[14] *Ibid.*, pp. 370-371.

[15] "Pepper-Spraying Drones Could Be Used on Unruly Crowds by Indian Police", The Guardian, 8 April 2015.

[16] Akshat Upadhyay, "Do-It-Yourself (DIY) Warfare: A New Warfighting Paradigm", Strategic Analysis 48, no. 1, 19 March 2024: p. 18.

[17] "On the Front Lines with Ukraine's Killer Drone Pilot", The Wall Street Journal, video published on YouTube, 14 October 2024.

[18] "How Are 'Kamikaze' Drones Being Used by Russia and Ukraine?", BBC News, 29 December 2023.

[19] Civ Div, "How I Make Kamikaze Drones", YouTube, 19 June, 2024.

[20] Maura Conway and Stuart Macdonald, "Introduction to Special Issue: The Practicalities and Complexities of (Regulating) Online Terrorist Content Moderation", Studies in Conflict & Terrorism, 19 June 2023, pp. 1–4.

[21] GIFCT is an NGO founded by Meta (formerly Facebook), Microsoft, YouTube and X (formerly Twitter) in 2017. See: GIFCT, "About," GIFCT Global Internet Forum to Counter Terrorism", last accessed 2 August 2025.

actors to develop preventive strategies and technical guidance. For example, following a mandate from the UN General Assembly and through a multi-stakeholder consultative process, the United Nations Institute for Disarmament Research (UNIDIR) created a self-assessment tool for states to evaluate their capacity to counter IEDs.[22] A similar model could address UAV threats, merging arms control principles with cyberspace governance to close existing policy gaps.

Partnerships among maker communities, universities, and the private sector should embed ethical guidelines and "safety by design" principles into drone development.

"Digital literacy programmes should equip youth with skills to critically evaluate online content, highlighting the legal and humanitarian consequences of weaponization."

Institutions can reinforce this by integrating ethics modules into the non-weaponization of knowledge, especially in engineering and science courses, fostering a generation of innovators aware of the risks and responsibilities of technological expertise.

[22] Bob Seddon and Alfredo Malaret Baldo, "Counter-IED Capability Maturity Model and Self-Assessment Tool", UNIDIR, 24 June 2020.

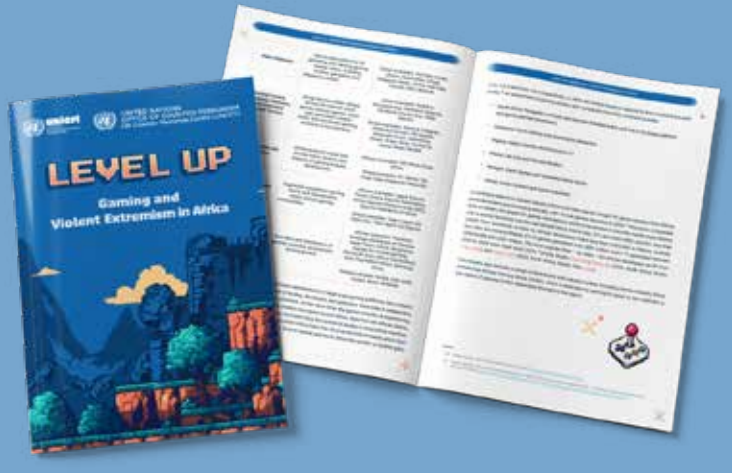
About the Author

Lara Maria Guedes Gonçalves Costa is a young professional working in the field of arms control and disarmament. She previously undertook the Graduate Professional Programme with the United Nations Institute for Disarmament Research (UNIDIR). Prior to that, she interned with the United Nations Office for Disarmament Affairs (UNODA) and the Stockholm International Peace Research Institute (SIPRI).

Lara also worked as an analyst at IBM BTO Business Consulting Services. She holds a master's degree in Security, Intelligence and Strategic Studies, jointly awarded by the University of Glasgow, Dublin City University and Charles University, and a bachelor's degree in International Relations and Area Studies from Jagiellonian University.

> **Governments should ensure that cyberspace governance discussions include the risks of open-source knowledge related to emerging technologies**

The new publication **Clicks, Links & Tricks, Oh My!** How Serious Organized Criminals Exploit Digital Trust Pathways examines how fundamental components of the Internet - domain names, uniform resource locators (URLs), and web traffic systems - are systematically manipulated. These elements, referred to throughout the report as "digital trust pathways", have become central enablers of a wide range of illicit activities. Strategically misused, they serve to facilitate, expand, and conceal criminal operations on a global scale.



Level Up – Gaming and Violent Extremism in Africa aims to deepen understanding of online harms in gaming spaces, particularly in the context of violent extremism. As gaming becomes increasingly social — especially through online mobile multiplayer titles with in-game chat — the potential for terrorist and violent extremist exploitation continues to grow.

The report **Right- and left-wing violent extremist abuse of digital technologies in South America, Africa and Asia**, jointly published by UNICRI and VOX-Pol, investigates the underexplored phenomenon of right- and left-wing violent extremist groups in the Global South and their abuse of digital technologies. As technology evolves at an unprecedented pace, violent extremist actors increasingly exploit digital platforms, posing complex and multifaceted threats to national and global security.

Download UNICRI publication