

Democratizing AI, the Good, the Bad, and the Ugly for the Security Environment

Article by **Sal Artiaga**

October 3, 2026



Introduction

All major technological revolutions start with enthusiasm. Later on, they become ordinary and, in the end, prove to be dangerous when put into the hands of people who never designed them, never fully grasped them, but who have learned enough to be able to use them. This is the direction we are moving in with artificial intelligence.

For many years, Artificial Intelligence (AI) was mainly the concern of governments, research laboratories, universities, and large technology companies. It was costly, complicated, and generally out of reach for the ordinary person. That situation has now ended. Today, AI tools are accessible to almost anyone with a phone, a laptop, and an internet connection. Some are free, others are inexpensive, and some require very little technical knowledge.

That is what true democratization means. Power, once the sole domain of institutions, is now spreading downward through society. It will offer huge advantages but also pose serious security problems. Experience has shown us, through the democratization of the internet, what happens when global connectivity becomes available to all faster than laws, norms, and institutions can adjust. It has provided the world with education, commerce, communication, and open access to knowledge. At the same time, it has given criminals,



extremists, hostile states, and conspiracy networks a global arena in which to operate. AI will do the same, but faster, to a greater degree, and with less resistance.

More Capability for More People (The Good)

AI democratization has a truly positive aspect that shouldn't be ignored. It can help small businesses compete, enable students to learn, help patients understand medical information, allow analysts to work with large quantities of data, and let citizens use tools previously available only to specialists.

It can translate languages, summarize documents, detect fraud, improve logistics, support disaster response, and help organizations identify patterns hidden within vast amounts of information.

Security experts can make use of AI to improve defense. Police authorities can use it to examine financial networks, spot trafficking patterns, and sift through digital evidence. Intelligence analysts can use AI to review publicly available information,

compare sources, and detect early signs of instability.

Those who defend against cyberattacks can use AI to monitor networks, detect anomalies, and respond faster to intrusions. There is also a basis for fairness since, for too long, technological advantage has been held by those with money, access, and institutional support.

By having AI available to everyone, smaller organizations, including underfunded agencies, civil society groups, journalists, and researchers, are allowed to take part in the information environment. What once required a large staff can now be done by a small team. **That is important. AI can act as a force multiplier for truth, accountability, and resilience when it is in the right hands.**

It doesn't mean that AI somehow transforms amateurs into masterminds since that would be an overstatement; rather, it does make mediocre performers more capable than they once were and enables mediocrity to scale, which is dangerous enough.

When the internet matured, all of these things changed. Criminals were then able to locate victims who were in other countries. Terrorist organizations could distribute propaganda to people worldwide. Hackers could exchange their tools, techniques, and stolen data. And conspiracy groups could radicalize individuals without having to meet them in person.

A small group of extremists no longer needs to set up a media department to produce propaganda, since AI can help create visuals, slogans, scripts, and translated material. A fraudster can carry out social engineering without deep technical knowledge because AI can help with tone, targeting, and repetition.

Criminals and Terrorists at the Lowest Levels (The Ugly)

The most unpleasant aspect of AI democratization is not how advanced state actors will use it; they already have the resources and skilled personnel. The genuinely disruptive change is AI's impact on the lowest levels of criminal and extremist networks.

A young gang member, an individual acting alone, a small smuggling operation, or a minor fraud ring can now access tools that help with planning, messaging, research, and deception. They can study their targets, imitate organizations, set up false identities, translate between languages, and produce content professional enough to deceive people.

Once more, the danger does not lie in perfection; the danger is in the large volume. Security systems are usually designed to detect amateur behavior. This includes poor grammar, clumsy messaging, bad design, inadequate research, and so on. AI removes these signs.

The scam appears neater. The fake profile seems more believable. The propaganda video looks more professional. The intimidating message sounds more official. The fake charity appears more credible. This situation presents a tough prospect for terrorism.

Radicalization could become more personalized since recruitment stories can be customized for the individual. A lonely, angry, or unstable person can be given content that seems to address their emotions directly.

Using AI, extremists can identify people's grievances and weave them into a narrative. Although this by itself does not cause



terrorism, it speeds up the process by which a grievance leads to mobilization. This is where the security situation grows more difficult, since the threat is not merely the formal organization but the motivated individual with access to machine aid.

The Internet Was the Warning

The fact that the Internet has become democratized should have warned us. Initially, it was hailed as a way to promote openness. People believed it could connect societies, spread democracy, improve education, and weaken authoritarian control. Some of these things did happen, but the negative side appeared quickly.

Cybercrime has become a global phenomenon. Disinformation travels as fast as emotion. Extremist groups have discovered safe digital environments. Foreign influence campaigns have exploited social media sites. Human traffickers have begun to recruit online. Counterfeiters have found buyers. Cartels have used encrypted communication and digital finance. The open architecture that enabled citizens also empowered predators.

The point isn't that the internet was bad; rather, the lesson is that technology ceases to be innocent when it gets involved in human conflicts. AI will follow the same pattern, but with even greater intensity; the internet enabled bad actors to connect and spread, while AI enables them to create and adapt.

The Security Environment Ahead

The future security landscape will be shaped by speed, deception, and scale, with security agencies facing more false information, more synthetic identities, more automated scams, and more targeted influence campaigns. The boundaries between criminal activity, terrorism, espionage, and information operations will continue to blur.

Transnational criminal groups will use AI to improve logistics, find more inventive ways to launder money, and detect enforcement weaknesses. Trafficking organizations could use AI-produced profiles and messages to deceive their victims. People who produce counterfeits may use AI to create more believable brands, documents, and marketing systems. Cybercriminals will use AI to boost both the volume and quality of their attacks.

Terrorists will use it to inspire people, recruit them, and communicate in ways that are

more difficult to spot early on. And I want to add that this is the light gray area; there is a much darker version of this.

At the same time, governments will struggle with jurisdiction, ethical issues, and the need for speed. Democracies cannot keep a lookout for everyone, since the threat landscape becomes more complicated. If they do, they would endanger the legitimacy they are trying to preserve. That is the problem.

Although AI-powered threats will require faster detection, democratic societies still have to function within the framework of the law, under proper oversight, and with respect for civil liberties.

What Must Change

The solution is not to panic since panic leads to poor policy; **the solution is adaptation.** All security organizations should build greater AI literacy at every level, not just in technical offices. Analysts, investigators, commanders, prosecutors, and policymakers must understand what AI can and cannot do; they should be able to identify synthetic content, question digital evidence, and think carefully about machine-generated patterns.

Law enforcement and intelligence agencies should also cooperate more with the private sector, since a large portion of AI-driven threats will pass through commercial platforms, banks, telecom companies, social media firms, cloud providers, and cybersecurity companies, each with an important piece of the puzzle.

Above all, security experts must realize that AI is not at the heart of the problem; people are. AI merely speeds up human intention and amplifies ambition, grievance, greed, and deception. The struggle will remain about behavior, networks, legitimacy, and trust.

Conclusion

Making AI available to everyone will change the security environment in ways we are only just starting to understand. It will benefit defenders, investigators, analysts, and ordinary citizens, but it will also empower criminals, terrorists, traffickers, fraudsters, and hostile networks. The internet has given humans the means to connect, but it has also provided a crime-ridden and extremist-friendly borderless environment in which to operate. AI will build on this existing foundation by making malicious actors not only faster and more persuasive but also more scalable, even at the most basic levels.

That is the unpleasant future. The tools are no longer being kept solely for the elite. The capability is spreading downwards. It can be remarkable in good hands and terrible in dangerous ones. **The security problem we now face is not just about controlling AI; that may be impossible. It is about understanding how it changes power, because when powerful tools become commonplace, the world does not go back to the old rules; instead, it adjusts, and so must we.**



M6