CONVERSATIONS ON STRATEGY

PODCAST TRANSCRIPT

Sarah Lohmann
"ChatGPT, Artificial Intelligence, and the Terrorist Toolbox"

Dr. Sarah Lohmann discusses the use of AI in terrorism, emphasizing its potential for both good and malicious intent. She highlights terrorists' utilization of AI tools for recruitment and accessing sensitive data, posing cybersecurity risks. Lohmann also touches on AI regulation efforts, disparities between regions, and the importance of innovation and transparency in AI governance. Global cooperation is crucial in mitigating security risks in the digital age.

Keywords: artificial intelligence, AI, ChatGPT, Perplexity, terrorism

E-mail usarmy.carlisle.awc.mbx.parameters@army.mil to give feedback on this podcast or the genesis article.

Stephanie Crider (Host)

You're listening to Conversations on Strategy.

The views and opinions expressed in this podcast are those of the authors and are not necessarily those of the Department of the Army, the US Army War College, or any other agency of the US government.

Joining me virtually from Germany is Dr. Sarah Lohmann, author of "ChatGPT, Artificial Intelligence, and the Terrorist Toolbox" from *Emerging Technologies and Terrorism: An American Perspective*, which was published by the US Army War College Press in April 2024.

Lohmann is a member of the full-time teaching faculty at the Information School at the University of Washington. Her research and instruction focus on information technology governance, cybersecurity, and emerging and energy technologies.

Welcome back to Conversations on Strategy, Sarah.

Dr. Sarah Lohmann

Thanks so much, Stephanie. I'm glad to be here.

Host

How concerned should we be about ChatGPT and artificial intelligence?

Lohmann

Well, chat GPT and artificial intelligence are in and of themselves neutral emerging technologies. That means they can be a force for good in the world or for terrorism, depending on the intent of the person using them. I've seen ChatGPT help my students better brainstorm and outline or more easily find sources for bibliographies for a paper they may be writing for my class, for example.

We can use artificial intelligence to help us stay ahead of cyber threats to critical infrastructure or even as part of facial recognition to help us identify medical disorders earlier or to help prevent crime. But at the same time, and this is what I address in my chapter, we've seen terrorists use ChatGPT to recruit or rally followers. But ChatGPT has seen several upgrades over the last year and a half and will now not answer questions about how to build a bomb or how to join a rebel religious group. Terrorists now actually have to use other similar large language model AI driven platforms like Perplexity Ask.

Sarah Lohmann
"ChatGPT, Artificial Intelligence, and the Terrorist Toolbox"

Another danger inherent in these kinds of platforms is that they make it easy for cyber criminals to create deep fakes or chatbots posted on the dark web to obtain sensitive personal or financial information. So, depending on how the tools are used, they can help prevent crimes or can make them easier to execute.

Host

Tell me about the AI toolbox terrorists are using for hacking weapons systems.

Lohmann

So, AI makes it easier for terrorists to conduct their crimes because they don't actually have to risk their own physical safety or have contact with their victims. They can sit behind a computer and use social media to access biometrics. There are plenty of high-resolution files out there for government officials and other high-profile individuals, and that makes it especially concerning that biometrics are often used for access to places of binational security value.

If a terrorist gets a hold of biometric eye or fingerprint data or voice patterns, that could allow them to access systems or labs or banks or even the stock market, which has drastic national security implications.

Secondly, we know that terrorists are already practicing using automated vehicles as weapon systems. That's because traffic guidance systems are connected through the Internet of Things and could be hacked to create loss of life if manipulation of destination occurs.

Host

That just reminded me of all the movies where you see the criminals changing

the traffic lights and all that.

Lohmann

It's actually a thing. It can actually happen.

Host

What are Latin American countries in the EU doing to regulate AI?

Lohmann

Well, we are very excited that the European Union's Artificial Intelligence Act is probably the most comprehensive regional regulation, and that was just passed this last month. It categorizes AI-enabled technology according to the risks they provide to health and to safety and to human rights. It bans remote real-time facial recognition, and it creates new transparency requirements for AI tools like ChatGPT.

This is basically going to have far-reaching economic implications around the globe because, and here's the rub, the transparency requirements also apply beyond the borders of Europe if countries have products they are selling in the EU.

Alright, let's switch over to Latin America for a minute. In 2019, the Organization for Economic Cooperation and Development [OECD] adopted its AI principles as the first intergovernmental organization to do so. And so basically working with the OECD, the Latin American and Caribbean countries have started creating their own ethical and human-centric approach to artificial intelligence. There's seven that are leading the way and that's Argentina, Brazil, Chile, Colombia, Mexico, Peru, and Uruguay. Most of those countries have specific objectives and specific outlines, basically for the responsible use of AI in the public sector. That means, really, where the rubber hits the road in terms of critical infrastructure, specifically now, they do still have a way to go in terms of cross-sector collaboration and procurement, as well as those policies on data and technical infrastructure. But at least they have strategies for these.

I think the aspect was the most surprising to me [was] that these countries are actually starting to lead the way. So, users of ChatGPT in countries like Brazil are already concerned that the new AI tool is violating the rules that they

already have in place, like the Brazilian General Data Protection law. So that Brazil law, if you remember, is a lot like Europe's privacy laws because it requires that the origin of data is clearly labeled and that any personal data that's used, like data entered into the Internet or used to train the large language model, is clear and accessible to users.

So, they're already wary and trying to make sure that the regulations that they already have on the books are abided by. Latin America was also a surprising case study to me because of the massive self-driving car market. In this case, I also want to mention Brazil. Brazil is the country with the most automated vehicles on the road in Latin America due to its infrastructure being interconnected. So, actually, Latin America has a projected compound annual growth rate from 2022 to 2024 of 28.5 percent. That is $3.75 billion.

This means that they have to actually refine those AI principles they came up with already in 2019. And they're doing that as we speak because they recognize the urgency of it. So, while we in the United States and in North America actually have no comprehensive regional law on artificial intelligence, basically, we're looking at it state by state in the United States. And then Canada is also looking at its own policies.

Almost every other region of the world has actually developed a comprehensive regional plan. So, we know the EU has; we know the African Union has, the G7, the G20. Then you have all these Latin American countries who have developed their own AI policies and their own regional policy. And we in North America are still piecing it together. So that was a real surprise to me that we have these 60 individual countries and all of these regions who have developed their AI policy. And Latin America is starting to lead the way in that area as well.

Host

Were there any indicators about why we're lagging so far behind in North America?

Lohmann

I think we want to put innovation first and let regulation come up with things. You have a lot of large tech giants who want to beat their competition, and they want to do as much as possible to get their products out there before the regulation catches up. That's just my personal opinion, though.

Host

What can NATO learn from how Latin America and the EU are regulating AI?

Lohmann

Well, NATO will also be looking at traceability, at reliability, and at governability because that's important as NATO protects civilian populations—specifically those that are impacted by terrorists' use of biometrics and self-driving cars. NATO can encourage good governance in addressing how sensitive conversations and Internet searches are stored and distributed over AI platforms, for example, or AI companies labeling false or damaging information as such on ChatGPT prompts.

Now, NATO is not a legislator. It's a defense organization. So, they can encourage that good governance, but the actual governing is up to the states. But they can continue to foster innovation and encourage democratic vibrancy that protects member state security through technology and that doesn't challenge it.

Host

Do you have any closing thoughts you'd like to share on this?

Lohmann

Yes, it's all not bad news. There's quite a bit of good news in there as well. There are a number of solutions for all the challenges we have discussed. So, when we're talking about ChatGPT, it's tightened its regulations and its allowable keywords so that many questions asked for nefarious purposes are no longer possible. Also, self-driving

Sarah Lohmann
"ChatGPT, Artificial Intelligence, and the Terrorist Toolbox"

cars are starting to install communication systems that provide warning to other drivers that your system is not functioning properly. It's also possible to install a manual override system.

So, there is a light at the end of the tunnel.

And I want to just say AI innovation holds a lot of promise. We just need to make sure we protect transparent and safe use of it.

Host

I love that we can end on a positive note. Thank you so much for joining me for this podcast.

Lohmann

Thank you for having me.

Host

Listeners, you can read the collaborative study at press.armywarcollege.edu/monographs/967. For more Army War College podcasts, check out Decisive Point, SSI Live, and a Better Peace.

Download this episode:

https://ssi.armywarcollege.edu/SSI-Media/Podcasts-Lectures-and-Panels/Conversations-on-Strategy-Podcast/mod/67381/player/581/audio/81362