2028 - Hacker-AI and Cyberwar 2.0+
(Securing our Future: Proactive Resilience through Separated Security Measures)
ISBN: 9798375252568

Final Thought

This final chapter is not the place to repeat problems we have or could have with Hacker-AI in international relations (i.e., warfare) or cybercrime. These final thoughts are about a future in which we want to solve problems with our security and what we can do better.

We must focus on getting our security problems fixed asap – if someone has concerns or sees problems with the proposed solutions. Please, make yourself heard; we need to hear about it asap. Still, discussions about details and contingencies happen during development.

However, we should urgently get software-related updates that create a (sufficiently) "incorruptible" layer of security below the Operating system. It will check and confirm that all security-related operations coming from the regular software (domain) are valid; deviations, i.e., actual rejections from the security layer, are suspicious and warrant some investigations by the software manufacturers or cybersecurity people. With AI, i.e., soon, these investigations will be fully automated, not just collecting relevant evidence. I believe Low-level-Security-Separation (L2S2) will be an incredibly powerful security contribution.

All security technologies must be made open-source. Open-source doesn't need to be free but open for constant audits and scrutiny.

We should have at least one dedicated open-source expert/developer community that focuses on countermeasures against malicious software, i.e., software that helps detect spyware and ransomware within the watchdogs of the security domain. These experts can also educate other developers on improving security in their custom solutions. Still, I don't advocate rewriting code or solutions but retrofitting them with a security separation layer.

There might be some resistance coming from cybersecurity professionals and businesses assuming that their business of selling anti-virus tools or firewalls will be diminished. But cybersecurity's mission is larger: protecting computer systems, networks, and their users from unauthorized access, use, disclosure, disruption, modification, or destruction. Cybersecurity will protect us against many cyber threats that are more custom. I can see how security experts help us against phishing or more subtle forms of cybercrime based on deception or impersonation. Security often starts with understanding what is worth protecting. Who knows what or where a customer's "crown jewels" are?

Protection could start with making someone aware that their personal or sensitive information could be stolen or compromised. Covert, unauthorized access to their user devices and networks should be prevented without making

a big deal of it; however, this could get tricky when there are trade-offs between security, availability, and convenience – that's when we need cybersecurity professionals most. Cybersecurity should be more of an adviser in security issues and not an operator. Security has to be automated as much as possible.

The biggest problem with software is intransparency about what it does. If this is already bad, it gets worse if adversaries can modify it. If we can trust that software can't be modified covertly, we must trust software developers and manufacturers – which is significant progress. Being a software developer (i.e., authorized to modify computer code) is a role that carries more responsibility than we acknowledge right now. We should keep the contribution of software professionals in a similar high esteem as that of medical doctors or lawyers. We have strong self-regulation that protects these professions from pretenders, fraudsters, and criminals. We need some (ethical, common-sense) rules for developers as well.

This book elaborated extensively on the misuse of AI in hacking, in Cyberwar 2.0, in extended forms of cybercrime. The risks are obvious. None of these negative applications can be prevented by legal or technical means. Also, no international accord will restrict a country from developing cyberwar weapons. The only defense is to have the IT infrastructure, and its ecosystem technically prepared to reject malware.

With the Internet, we have the tools to update our defenses much faster than we are doing it. Currently, it seems that the attacker has an advantage. No law of nature makes us accept that assailants have an attacker's advantage. We did this to ourselves; we made defense reactive to attacks. As long as the environment is new, dynamic, and unfamiliar, being reactive is ok. But we should grow up, go proactive, and set the rules accordingly.

Security in all other technical domains (product safety, building code, or aviation safety) is less forgiving in dealing with failures. Cybersecurity should not remain a branch of security in which excuses are sufficient to avoid accountability.

We are late in implementing better security. But there are no signs yet that we are too late. We should accept our luck and not gamble it away by hoping that we have even more time or luck by doing nothing or too little.

If anyone among you readers has the resources to make a difference, then do it quickly.

References

In the preface, I told the story or the drama of being hacked. Files were deleted, etc. I needed to decide to get these ideas out asap.

I knew about the deficits – and you are now looking for references, which tells me you are an expert. This book it's not the final word on Hacker-AI or cyberwar 2.0+.

Now, I consider this situation an opportunity to get in touch with experts and pros who will hopefully give me some feedback on this book for the next edition.

If you think I should include certain articles, books references, or other information or arguments, then please let me know – **2028@nogostar.com**

As a thank you for your valuable input and feedback, I will send you a PDF version of the new edition in response to your eMail.