2028
Hacker-AI and Cyberwar 2.0+

Securing our Future: Proactive Resilience through Separated Security Measures

Erland Wittkotter , Ph.D.

ISBN: 9798375252568

DEDICATION

For my love S.M.O.
and to Rolf, Anke, Jerry, Ross, Rose, Daniel, Fabian, and Charles
without them, I couldn’t have finished this book

Contents

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

Preface

There was some drama around writing this book.

If you expect a topic introduction, the purpose of writing this book, or background on the subject matter, please go to the next chapter, "Introduction". I take the liberty to write about what happened recently.

I don't have all the puzzle pieces together, and I don't even know if all found pieces belong to the same game or picture. So I restrain myself: I won't speculate what has happened in the shadows. I had the distinct impression that someone wanted to tell me something without talking to me.

Being attacked or hacked should not really be a surprise. I am writing a book about hacking, inadequate cybersecurity, AI used to exploit vulnerabilities, etc. So, why am I surprised? Well, it didn't happen to be before.

But yes, I got hacked, and some documents were deleted, even from this book and other research. Potentially they were even stolen. But having (seemingly targeted) files get deleted, well, that was scary, not from the damage point of view, because I got everything restored from my backup. However, some screenshots I made from suspicious apps using my security tools were gone (not even undelete got me anything). FYI: I am intentionally vague on several details.

One day before, I found components on my system that were using computer resources, and I could not assign them, so my hunt started. Actually, I love doing that; whenever I do that, I learn a lot about computers' internals. So, I made some screenshots that I wanted to follow up on; but they were gone, and the suspicious software from which I made some pics was gone as well.

After the deletion of these files, I knew something was going on. So I beefed up my security significantly. What I exactly did, I don't want to say – only so much: I used a hypervisor to create multiple security zones that were strictly separated from each other and had their resources, access control security, and encryption. Additionally, I have had a couple of performance monitors telling me when something tries to get more resources than expected.

I am grateful for these tools and the work others did to make them incredibly useful: So a "Thank You" to the open-source community who created awesome tools that keep us safe. And yes, I have anti-virus suits, etc., but they were not helping me – (hmmm) why is that?

A few days later, I saw a large file after my lunch break; it was ransomware (no more details here). Events that were repeated after many breaks – or longer pauses I took. I removed them, but it seems attackers left a downloader. I found

something recently and did a low-level removal, i.e., external drive and low-level console). Now, I will wait and see because I have only limited time I can use for chasing ghosts. So who knows, maybe something is still on my system.

Also, I would have expected that someone would have come up with a "Deadman Publisher" software, i.e., publishing some content/research after a person is "incapacitated". But no, so I quickly got into my Python environment and did a quick and dirty on some features I needed to protect my research. Well, the first version (tested and working) was not working properly (I found out later). This means my research would not have been sent out in 10 days but in 10 years after my (last) check-in. I only found the problem accidentally – It was like: "Oh, what's that?". Still, I am not sure: Was it my fault? Because I was a little bit sloppy with my security working on that solution, I decided to improve my security measures around the "Deadman Publisher" as well – if it really works: I don't know; I didn't need to use it.

Other events were also headscratchers, but coincidences are not causalities. I see more because I try to be more aware of my surroundings. And in some weird ways, it gave me more insight into the development under conditions in which we don't know if malicious actors are trying to sabotage the work of developers. However, I won't say any of these events are causally related to writing this book.

After detecting the hack, I knew I needed to finish this book quickly. There is one other thing I pursue that might (theoretically) be related to these hacker events - I doubt that (but I can't know).

However, I concluded that my main path to make myself less interesting for whoever is interested in me is to finish and publish this book asap. I have eliminated (at least) one possible reason.

So I know there are a few things I should have done, like creating an extensive list of references, making sections more engaging, or have hired someone who would have extensively edited the book. Ok, I didn't do that. If you are reading this book now, you won't care if I promise this for the next edition or the next book.

I included the content that I believe needed to be out in the public. That my target audience receives my message is not in my hands alone, they need to be made aware – but chances are that the message could spread to the ones who should read this.

I hope you agree that this book is now at a stage where it can and must be published.

I am thankful for positive (and even critical) feedback, and when permits, I will respond: **2028@nogostar.com**

If you are an expert in one of the relevant topics, I will enjoy reading your comments.

And, if you are a reader with the resources to make a difference, please read this book, consider what you can do, and then do it quickly.

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

Introduction

How do you envision the future of cyber warfare? Better spyware or larger denial of service attacks on some web servers? These are past concepts; the future could be much scarier if we are not vigilant. Or do you want to be prepared for a cyberattack of unprecedented scale and sophistication? This book, "2028: Hacker-AI and Cyberwar 2.0+," explores the chilling reality of AI-powered hacking and the potential consequences for our privacy, freedom, and security.

The Pegasus spyware, developed by NSO Group before 2016, is old technology and just the tip of the iceberg; there are other cyber mercenaries commercially active in this business. As old software vulnerabilities are fixed, new ones are constantly being discovered and exploited. But what if more vulnerabilities are detected must faster? And what if the next generation of malware is more advanced, pervasive, and undetectable?

Imagine a world where AI-powered malware can infiltrate any system, technology, or device and filter through the noise to find the most valuable information before reporting it. Even small teams of spooks could manage and direct large malware armies. The stakes are high, as this type of malware could grant its operators unparalleled IT supremacy and potentially change the balance of power in the world.

But it's not just about the potential for cyber warfare; AI-based surveillance combined with social scoring systems could also lead to a society controlled by unaccountable, even criminal elites. The book 2028 explores these issues and offers concrete, common-sense solutions to make our cyber world safer and more secure. It's not enough to report a problem or predict a new variation of dystopia but to understand what must change, where we need to take action, and how to make a difference.

Don't let the future catch you off guard. There are major problems that you need to see, and we must fix these issues together asap. I hope you will see cybersecurity more personally. We can take control of our cybersecurity before it's too late. Are you waiting for another Pegasus to infiltrate your device, steal your data and take you for a ride? We need to take action now and demand that cybersecurity be treated as a common human right. Let's make no mistake; the stakes are high. If you believe this to be an exaggeration, it is only because you have not yet fully grasped the gravity of the issue. Unbridled surveillance has the power to strip away human dignity and turn entire societies into mere puppets.

Why this Book

Cybersecurity is a critical concern for individuals, organizations, and governments. The increasing interconnectedness of our world through technology has exposed us to new threats to our privacy, freedom, and security. Malware capable of exploiting every feature of our devices and systems is a reality. The potential for hackers and criminal organizations to harness the power of artificial intelligence in their attacks is a looming, even urging threat.

The proliferation of security-threat-related technologies, i.e., the ease of access to tools and knowledge required to create and deploy malware, is a significant concern. The possibility of giving private and criminal organizations the power to cause significant damage and disruption is akin to giving them tools as powerful as nuclear weapons.

We must demand that cybersecurity is taken seriously and measures are implemented to make our digital world safe and secure. Security should not be considered an optional feature but a fundamental human right. We cannot allow software and technology to be covertly manipulated by adversaries and used against us. A different approach to cybersecurity is needed, one that prioritizes security, making it easier to implement and maintain while still having it almost unnoticeable. With the right approach, we can create a safer and more secure digital world for all.

Audience

You may wonder who this book was written for. And, have I considered if you have the knowledge, background, or patience to read this? However, you don't have to be a hacker, cyber-warrior, or IT expert to find the topic relevant.

This book is written for a diverse audience of security professionals, politicians, military leaders, academics, and industry experts interested in understanding and improving cybersecurity. It provides valuable insights and strategies for those who may not have a background in computer science but are responsible for ensuring national security and protecting against cyber threats. Additionally, the book will offer new perspectives, like paradigms, that will lead to new practical solutions and technology implementation or proposals for cybersecurity professionals, system developers, and open-source enthusiasts. (I trust they will figure out the details I didn't include to keep it enjoyable for the non-techs.)

I hope to stimulate discussions within IT membership organizations to be part of enhanced self-regulation beyond technology standardization. IT professionals hold a position of trust and are responsible for their actions. (Unethical involvement in cybercrime should disqualify IT professionals from being part of this industry; this should rightfully tarnish their reputations publicly.)

I hope the book is an interesting and useful read for software entrepreneurs, CTOs, and investors looking to understand the current state of cybersecurity and potential opportunities. I didn't include a comprehensive introduction to

cybersecurity. Instead, it is about security challenges, practical solutions, and strategies to improve security as quickly as possible.

Author

I am a physicist, mathematician, and entrepreneur with a background in software development and a passion for Python, a popular computer language often used in data science and machine learning. For nearly 25 years, I have been interested in cryptography, cybersecurity, and system programming (including Linux Kernel, of course). I have studied many low-level technologies and got some experience in reverse code engineering, which helped me to understand what hackers and AI could do.

Three years ago, I intensified my research on the potential threat of autonomous AI, an interest I have had for many years. I returned to reverse code engineering, cybersecurity, and cryptography. The idea was to define and utilize security measures to defend us against advanced AI and apply these tools to combat cybercrime and cyber warfare perpetrated by humans and governments.

I had not been aware of the Pegasus project publications in July 2021 until recently, as I had been focused on other deep tech issues. However, upon studying the short-term implications of AI in hacking, I feel compelled to make clear statements about my convictions that guide this book. I strongly advocate for the rule of law, personal freedoms, and holding cybercriminals accountable. I am opposed to using cyber warfare to destroy or control other countries, surveillance, and a society controlled by an unaccountable elite.

Main Takeaways

Hacker-AI is AI-assisted hacking. Other terms for it are AI-power or AI-driven hacking. I have chosen the term Hacker-AI to emphasize the role of AI in hacking. It can assist humans, but AI could have also a more active or independent role as an automated tool or resource used by the human hacker.

Here are a few key points that I will make in this book:

- Computer vulnerabilities result from software complexity, and current OS security is insufficient to protect our devices.
- Software can be modified covertly; it isn't easy to trust tools. Attackers can often vanish unidentified. Secrets are unreliable in defense, and even defenders can be turned into traitors.
- Hacker-AI, which generates undetectable and irremovable malware, is a new challenge. It is uncertain who will develop and use it.
- Hacker-AI can generate malware to steal data, mass-scale surveillance, covertly communicate among user devices, and design/execute misdirection and deception campaigns.
- Cyberwar 2.0 uses Hacker-AI to overthrow governments in targeted countries; it's much less costly than conventional warfare. It could be

used in scenarios such as China annexing Taiwan or the US assisting the Russian opposition in transitioning to a post-Putin country.

- Although the experience of being in a Cyberwar 2.0 cannot be compared to the horrors of a conventional war, the long-term consequences for people's freedom and life can still be severe.
- Cybercrime 2.0 includes disrupting eCommerce, money laundering, manipulating law enforcement, and even cyber jailbreaks where malware taints or creates confusion with evidence.
- Proposed technical solutions for Hacker-AI include developer accountability, hashcodes, and separating security and regular tasks. New cybersecurity paradigms are suggested; we need quick low-level security separation (later called L2S2) and an expert development community.

This book was written to stand out from others by not just highlighting a problem but offering solutions and direction for improvements. Rather than simply reporting on an issue or placing blame, "2028" provides a new perspective that leads to practical and common sense solutions for creating more secure computer devices and a safer world for us humans using software-driven technologies. After reading this book, I hope readers will see cybersecurity as a fundamental human right essential to protecting our freedoms in a digital age.

Why 2028? Because I hope we have that long to do something about Hacker-AI (i.e., when we start immediately with some common-sense countermeasures). By 2028, we could (hopefully) declare that we dodged bullets from Hacker-AI, Cyberwar 2.0, or cybercrime. This is not a prediction; it is an ambitious goal.

Chapter Overview

For some, this might be boring, but here is a brief overview of what you can expect in the following chapters. In short, the first 9 chapters of the book discuss problems and harmful capabilities of malware, Hacking-AI, cyberwar, and cybercrime, while the last 5 chapters focus on solutions and strategies for addressing these issues. (Including what can be done when it is too late). This structure highlights the negative aspects of the problem and then provides a balanced perspective by offering solutions and strategies for addressing these issues.

Chapter 1 scrutinizes computer vulnerabilities. We need to go after the (real) reasons behind cybersecurity issues, like software complexity or how we use interfaces in components to make developers' lives easier – but inadvertently, it's getting easier also for sophisticated attackers. We expect developers that they understand and avoid vulnerabilities, but realistically, without robust OS/device security (even more than what Apple currently offers). No OS can promise to defend against surveillance or misuse (if they do, this is marketing).

In chapter 2, we go deeper into the reasons for computer vulnerabilities. 12 problem categories that contribute to these vulnerabilities, like the potential of covert backdoors or the negative impact of complexity on security, are identified. Without having all these problems solved, we won't have security. Amazingly, cybersecurity professionals know that but have given up on solving it. These 12 problems will be our challenge in which the proposed solution must show its worth.

Next, we will explore the use of AI in hacking, i.e., gaining unauthorized access to systems, stealing sensitive information, or causing harm to computer systems. We look at how AI-generating malware (i.e., malware from Hacker-AI) could hack other software and how undetectable and irremovable malware like Cyber Ghosts and Cyber Devils could irreversibly undermine our security.

To understand the basic features of Hacker-AI and its capabilities, we examine in chapter 4 how it is utilized in cyber warfare, or Cyberwar 2.0, as I will call it. I anticipate that Hacker-AI-generated malware can locate all hackable devices through reconnaissance, establish initial beachheads on every device it finds, and increases its rights/permissions (i.e., become sys-admin) to conceal itself on attacked systems. It will likely use (traceless) human communication channels/tools for its own secret communication. The malware will act as a masterthief stealing protected data and/or as a surveillance tool to monitor and report relevant user activity and aggregated/condensed data only.

In advanced features, chapter 5, we examine how Hacker-AI utilizes undetectable software, such as Cyber Ghosts and irremovable malware (Cyber Devils). We explore how Hacker-AI could create exclusive backdoor features, allowing access only by its original creator. I discuss how a Cyber Patsy-Designer can help attackers to blame others for a cyberattack and manipulate the narrative of a cyberattack by misdirecting the investigators and the public.

The high cost of resources, efforts, damages, and losses is a natural deterrent for countries to wage conventional war. Military actions mainly aim at destruction and disruption, including current forms of cyberwar. However, Chapter 6 explores how AI-generated malware can prevent/avoid damage in Cyberwar 2.0; it could be used for covert and rapid government overthrow or regime change. We examine the undetectability of these actions and the ability to predict successful outcomes through simulation. Waging Cyberwar 2.0 could become a smart (business/profitable) decision; there is no deterrence to prevent that from happening.

In Chapter 7, the phases of Cyberwar 2.0 are analyzed, starting with covert surveillance and extending to post-conflict considerations. Cyberwar 2.0 simulations could take into account potential unexpected events or variations. With timely feedback via the Internet, the fog of war is eliminated within cyber actions. The scenario of China's annexation of Taiwan is a possible first example of this type of warfare. The use of Cyberwar 2.0 by the United States to achieve a smooth transition to a post-Putin era in Russia is also discussed.

In chapter "8. How is it to be in a Cyberwar 2.0", I want to show the effects of Cyberwar 2.0 on individuals and society. I highlight the stark contrast between conventional wars' devastation and cyberwars' consequences. This chapter provides the perspectives of those affected by Cyberwar 2.0, including the general public, intimidated officials/recruitees, security officers, the government, and the attacker.

Chapter "9. Cybercrime 2.0 - Scenarios" explores the next generation of cybercrime and the effects of advanced technology on it. Hacker-AI-generated malware can target individuals and organizations, including stealing user credentials and encryption keys, including causing major damage to eCommerce and online banking. Additionally, cybercrime 2.0 can be used in large-scale money laundry operations; malware could manipulate legal proceedings, leading to Cyber Jailbreaks (i.e., guilty parties are acquitted because the evidence was attacked/manipulated/tainted). Hacker-AI could also be used to create new identities for criminals or remove stains from their resumes.

In chapter "10. Cyberwar 3.0 - Start of a Solution", I introduce Cyberwar 3.0, which uses AI/autonomy beneficially. Cyberwar 3.0 is a data/drone operation that uses non-lethal autonomous drones to target weapons and only individuals who threaten others with weapons. These drones target gun barrels in artillery, tanks, rifles, and handguns by using chemicals or metal pieces to destroy, e.g., the barrel's bore, making it dangerous for the shooter and rendering the weapon inoperable. Microdrones (3 to 5 cm in diameter) would be mass-produced; they could be retooled with different weapons/capabilities. Cyberwar 3.0 weapons, like any other weapon with software, must be protected and hardened against cyberattacks to prevent them from being controlled by cyberterrorists.

In chapter 11, I propose a series of technical countermeasures to protect against all major threats by Hacker-AI, which exploits vulnerabilities in software and manipulates systems. Current cybersecurity solutions are insufficient because a single vulnerability can invalidate all other measures. I recommend six countermeasures to protect against Hacker-AI, including (a) self-regulation among developers, (b) by default hashcoding to make software easily identifiable, (c) separating/duplicating security operations from regular operations, (d) protecting keys from theft, (e) protecting crypto devices and security components from misuse, and (f) automating low-level security to react to global Hacker-AI threats instantaneously.

In chapter 12, I apply the proposed security solutions to the 12 software-, attacker-, defender-, and crypto-related problems discussed in Chapter 2 and show how they are solved. To effectively address these cybersecurity issues, we need to take a comprehensive and low-level approach, using redundancy to have a "security overkill" that is also unnoticed by users and most developers. I show that the proposed solutions make security as simple as possible but not

simpler. We can uncover previously covert security-relevant activities while reliably identifying the attack's source. I discuss new paradigms for cybersecurity, suggesting six main points: 1) distrusting CPU/OS and 2) separating security-related tasks from regular tasks; 3) validating local code using hashcodes and 4) creating developer accountability; 5) preventing key-cleartext disclosures by using protected CPUs for key processing; and 6) establishing multi-unit security by having security components guard each other.

In Chapter 13, a three-phase approach called Low-Level Security Separation (L2S2) is proposed to address the urgency of Hacker-AI and Cyberwar 2.0. The sooner we have advanced security from security separation (L2S2), the better. The suggested approach involves developing a redundant (1) low-level software solution, (2) independent/retrofittable hardware components (watchdogs), and (3) incorporating phase-2 watchdogs in storage/network hardware by default. The goal is to implement L2S2 technology in as many devices as possible (and as soon as possible) to protect against advanced malware threats. For accelerated deployment, the development effort should be done in an open-source expert/developer community (www.nogostar.com) that educates also developers on advanced security issues. The main problem with the development is that malware from Hacker-AI (once it exists) could sabotage all efforts to deliver countermeasures. Therefore, if we start too late or are already too late, we may fail to get reliable security software or hardware.

Chapter 14 discusses the concern of inadequate preparation with technical countermeasures against Hacker-AI. To address this, I propose civil defense measures to be implemented during and after Cyberwar 2.0 events. For unprepared countries, the suggested strategy is officially announcing that the country is under cyber-attack, supported by sufficient proof. Additionally, it is proposed to assist those threatened by the new regime to leave their homeland when there is no possibility of stopping the government from being overthrown.