ISBN: 9798375252568

9. Cybercrime 2.0 - Scenarios

When introducing Cyberwar 2.0, I used the 2.0 label to describe a next-generation cyberwar concept that hasn't yet had a long history. In saying this, I am referring to the cyber aspect, not warfare. War is probably as old as humankind and already went through 100s of iterations. Something similar can be said about cybercrime. I refer also to cybercrime as criminal activities involving computers or the Internet, such as hacking, phishing, ransomware, identity theft, and other illegal activities that significantly threaten individuals, organizations, and governments.

When I use 2.0, I generally mean next-generation technology and its advancements as a qualitative difference from current or past applications. From next-generation technology, I expect that it is more advanced, powerful, efficient, user-friendly, and capable than the current or previous-generation technology. Some would expect that it is also more sustainable, safer, and secure, but that is not the case with Hacker-AI. Therefore, I use 2.0 or next-generation as a label to signal a significant change to current capabilities.

Speculations on next-generation cybercrime evolve from extrapolations to more advanced technologies and tactics, such as Internet of Things or IoT-based attacks, cloud-based, 5G-based, voice-based, blockchain-based, biometric-based, smart city-based, and even automobile-based attacks, etc. Cybercrime will change because of changes in the underlying technologies and adapt to vulnerable individuals and organizations under new conditions.

Hacker-AI could significantly change the application scope. We know how powerful spy features on smartphones can be from Pegasus spyware. An entire cyber mercenary industry is working on governmental trojans and software that could harm or spy on people. Pegasus created a scandal because its manufacturer was not overly picky in accepting some questionable customers using spy software against journalists, human rights activists, and dissidents. However, (professional) criminals, i.e., the ones that still enjoy freedom, use (pre-paid) burner phones, not smartphones.

The problem is much deeper than Pegasus or having an unregulated cyberweapon industry that develops spyware or other malware for whoever can pay for it. The problem is that we have a technology platform allowing spyware or other malicious features to be covertly used against its device owners and users.

The development of malware can be criminalized, but that is not sufficient. Criminals can work from anywhere; at some point, they may have the tools to wash their past clean. Hacker's lessons drawn from Pegasus differ from most others: What can be done to leave less or no data traces behind? Why was Pegasus so careless in being detectable by data forensics? Why did they not detect that they were detected?

Regulating the spy- and malware industry will not affect or even bother people who don't care about rules and laws. There is a huge financial incentive to continue developing malware. In short, drug trafficking or street crimes makes you money, mostly cash, but suspicious cash gets you quickly in jail. Soon, cybercrime could make criminals more money, get it even laundered, and get people out of jail.

Having advanced hacking tools is not a crime. The unauthorized use of these tools might be a crime (in some countries), but removing data traces automatically that these "tests" ever happened is probably not a crime. Developing features that have dual-use applications in hacking (and within tech support) might be regulated in some countries, but discussing it and doing some engineering study on it is all covered by freedom of speech and research. Hackers could get in trouble for being paid by criminals. But these criminals could form legitimate software security companies and fund them through laundered/legal money.

Regulating these kinds of technologies is a bad joke - if the regulation involves serious enforcement, developers would need to accept 24/7 surveillance. The knowledge for developing Hacker-AI features is freely available. With enough money, advanced hacking technology will end up in the hands of criminals sooner than later. The advantages of using Hacker-AI are simply too steep. Once the Hacker-AI milestone is taken, applying malware in Cybercrime 2.0 activities has zero barriers.

There is still deterrence from being criminally charged, convicted, and jailed for being a cybercriminal - but who said that the judicial system is immune against hacking attacks? US law enforcement is chasing criminals worldwide, with tenacious investigators and prosecutors going against cybercriminals like Anonymous or Dread Pirate Roberts (Ross Ulbricht) from Silkroad. Still, in their backend, serious vulnerabilities are not addressed sufficiently, as discussed below.

Where could we Expect Cybercrime 2.0

With Cyberwar 2.0, I have identified its main application: regime change and overthrowing governments. In Cybercrime 2.0, I see multiple applications of Hacker-AI that I will describe in the following:

(1) Hacking eCommerce/online banking by stealing user credentials and encryption keys

(2) Money laundry by helping criminals to legalize their illegally acquired cash or questionable bank accounts safely

(3) Manipulating legal proceedings and actions, including digitally triggered jailbreaks

(4) Creating new identities or cleaning someone's past

(5) "Cyberwar 2.0 as a Service" by offering disgruntled oligarchs help in changing their home country's leadership.

There are many more methods of using Hacker-AI in Cybercrime, and a few additional methods are being mentioned under the above categories in the sections below.

All the above Cybercrime 2.0 applications are very likely serious crimes. And criminals know: it is not what someone did but what the government can prove beyond any reasonable doubt. Doubt is what Hacker-AI will create. It will even create doubt that Hacker-AI even exists. So what will/can the government do? Accept that criminals are innocent patsies? Let them go?

The goal of this chapter is not to give criminals ideas on how to play the system but to show that the current flaws in security are unacceptable. If Cyberwar 2.0 is not scary enough, be prepared to live in a world of Cybercrime 2.0.

(1) Cyber Masterthiefs and Disruptors of eCommerce

eCommerce, online banking, and online stock trading are industries in which daily (almost) billions of transactions are created, making 10s of trillions of dollars in transactions annually. Getting a small cut from that is worth 100's of billions of dollars. There are estimations that cybercrime damages could add up to 10 trillion dollars by 2025. The estimation for 2020 (by Gartner) was one trillion dollars in damage due to cybercrime.

Why is so much money at risk? Because eCommerce is based on the trust in underlying encryption used in all business transactions. The encryption algorithms/methods are probably impeccable, but the keys could be stolen by malware from the software implementation within the crypto components. Without key secrecy, there is zero security in the business transaction. We cannot even detect that we have been robbed after it's too late. With sophisticated malware in action, we would not know what transaction failed or scammed us.

It is explained in other sections of the book, so this is just a reminder. If the technical standards SSL (Secure Socket Layer), TLS (Transport Layer Security), HTTPS (secure Web/HTTP), and many less prominent support standards are being hacked - and hackers get their fingers on the encryption key, then there is potentially only one additional protection left: Two- or multi-factor authentication (2FA/MFA) using an additional device.

2FA/MFA confirms user's identity by something the user has, like a phone or security token, or something that only the user has, like his fingerprints or voice. The main idea behind 2FA and MFA is to increase security by making it harder for attackers to gain access to users' accounts; the attacker would raise suspicion because the user is asked for a second form of authentication, then 2FA/MFA does its job.

Cybersecurity assumes that eCommerce's security is still holding, particularly if 2FA or MFA is used. Unfortunately, there are multiple threats to 2FA or MFA, like hackers, who are already on the second device, hackers controlling and manipulating the underlying terms of the transaction, or software being deceitful in the output to users. If 2FA/MFA fails regularly, we will lose trust in eCommerce and Online Banking soon after.

Hacking eCommerce, online banks, or manipulating portfolios in stock trading accounts is not a victimless crime. Big corporations, banks, or the government will not absorb the damages and keep the consumers unaffected.

Also, it should not be expected that many robin hood apps will steal from the rich and give it to the poor. I don't want to predict what features criminals will use, but getting money is just one form of being paid. There are other ways to benefit criminally. Products and services could be ordered but paid for by someone else entirely unaware of that. The problem is not just like a misused credit card; this could get much deeper into how reliable cloud servers can operate their online businesses. If online businesses are hacked, would the company even detect that? Can businesses trust their algorithms, their servers, or their data?

Trust is extremely critical. It's the foundation upon which online transactions are built. Trust has many layers: security, privacy, reliability, authenticity, and reputation. Personal information and financial data must be kept safe/secure, not shared or sold to third parties. Also, delivered products or services must be as described, and issues related to deliverables should be resolved quickly and fairly. Many small details within transactions on both sides must be stated truthfully, executed with integrity, and protected from malicious modifications from the outside.

Example: If a package is not delivered, was this because it was not sent out or sent to the wrong address (e.g., got a wrong address label attached) or was sent via a shipping container that got lost on the high sea or was stolen or the package was misdelivered or taken by the delivery guys, or was it delivered, but the receiver denies it. All commercial transactions are complex and prone to error or fraud; processes are established to reduce the probability of failures or fraud.

If problems happen, people need to get involved, which is expensive. Solving exceptions doesn't create confusion because there are many "what happens when" rules. Even fraud, accidents, and potential sabotage are factored into the price of goods and services. Businesses are usually managed and orchestrated with software quite efficiently. Less used features are often a goldmine for vulnerabilities.

There is currently not really a sudden threat of having vandalizing malware. Vandalizing software is intentionally causing damage to computer systems or networks by deleting/corrupting data or rendering systems inoperable. That software may exist for revenge, but cybercriminals are not using it yet. Instead, ransomware is used to give victims a choice between payment and continued operation or significant losses from disruption of business operations.

A sicker version of malware is to offer significant disruption of eCommerce or commerce-related activities as a service. Criminals could provide a paid "Revenge as a Service" business in which hints and background information on victims are handed over to perpetrators. Why paid? Because some would even pay for revenge. It is known that many people don't like each other, and it is not outside sick human-to-human behavior to give precise hints on personal or business details of enemies to criminal hackers who could then damage that person.

In the extreme, it is conceivable that wealthy criminal oligarchs are going after each other and driving their business into the ground or having their enemy lose a large amount of money. Because this is not a one-way street, victims could retaliate. It is, therefore, probably more a serious crusade to put someone completely out of business, which means revenge may turn more into a "Bankruptcy as a Service".

While writing this book, I read about Sam Bankman-Fried, who denied any wrongdoing in the crash of his FTX crypto-empire. Without knowing any details firsthand in this case, I know enough about business to say: businesses and their controls are complex. Management skills are used to simplify organizations, but external circumstances and the business/tax environment demand additional complexity. Modern businesses must be run by professionals who are expected to know what they are doing. There is no pocket calculator used when controllers check the books. Paper-based invoices or contracts are eventually being checked, but it is mostly about software and its automated triggers.

Although Hacker-AI is designed to explore low-level vulnerabilities, its malware could also reveal how a business is represented via internally stored data and how triggers help its operators to detect problems. Some of these triggers could discover manipulations; others look for unexpected trends or insufficient authorizations. Missing triggers might have caused FTX's downfall. But hackers in real attack situations could bypass software triggers, initiate transactions, and create track records that could blame others for what the hacker has done. Once electronic manipulations are done covertly, i.e., without leaving evidence, the situation has turned into accounting irregularities which could bring down even business icons when guided by smart people who are being paid for these kinds of hit jobs.

Consider this a warning to the super-wealthy. With Hacker-AI and Cybercrime 2.0, they are not untouchable. Lawyers won't help them; they are probably on their own. It's better to say it now: Everyone could be brought down when Hacker-AI is around. Unfortunately, that is not a hyperbole.

If anyone would tell me, Hacker-AI could not get that bad. Unfortunately, the situation is that without computers and IT devices having sound technical safeguards, yes, it will be that bad.

The loss of trust in electronic business transactions and the integrity of business processes could have catastrophic consequences on customers and financial markets. Most criminals would be affected by these market manipulations as well. Still, it may not require more than a handful of professionals/ criminals to start a heist that could make them billions.

(2) Money Laundry

"Never enough" is a typical mindset of many criminals until they are caught with too much unaccounted cash and traces that could link them to criminal activities. Having cash and no reasonable explanation of where it came from is probably the most serious problem for criminals. The money must be laundered so that it appears to come from legitimate business activities. It must be taxed before criminals can use it for legitimate purposes or purchases.

I saw videos on youtube about "ex"-criminals talking about burying cash in boxes and bags within their garden or hiding it within the attics or walls of their real-estate properties. Having large cash amounts is often more a curse than a blessing. Officials, even politicians, receiving large bribes have a problem getting the cash into their accounts due to limitations on cash amounts that banks accept without reporting it. As long as cash is not being laundered via legitimate businesses, that money is almost useless. Anonymous cooperations and offshore businesses help a little, but tax reporting on global income and business ownership could make illegal money a huge liability that could even give someone jail time without being convicted for the crime that provided that money.

Based on stricter banking and taxation rules, money laundry is probably a bigger problem for criminals than receiving more money from existing or new streams of cash. Smart criminals think of exiting the criminal world as soon as they have earned large amounts, potentially even generational wealth; for them, crime is a business. Reducing the risk of being caught is often more important than making more money.

I studied a couple of methods on how money laundry is currently done, and I can also see the problems with these methods. This book should not educate anyone on this topic and help them create a business around it. Therefore, I would like to leave it as a hypothesis that malware from Hacker-AI could be used to control and execute money laundry on a much larger scale than done now. Moreover, I believe the risks for criminals could be reduced and potentially eliminated. The incentive of having access to money and avoiding jail for tax evasion is so significant that I consider the technologies that facilitate money laundry killer applications for Hacker-AI.

Getting the Hacker-AI that could make laundering money much safer for all involved would be worth almost any amount. However, there is a catch: The cybercriminal offering this service must be honest enough not to steal the entire laundered money. And what was the saying: There is … honesty among thieves. However, stealing money is no news in Cybercrime 2.0. Maybe criminals will have capital punishment for these indiscretions.

Cryptocurrencies could help cybercriminals feel safer after committing a crime and receive money without getting connected with a specific crime. The bad news: cybercurrency is not anonymous. Keeping it in wallets that are connected to them is dangerous. Criminals must even launder crypto before they can fully use it. And money laundry, even of cryptocurrencies, is risky for everyone involved.

It doesn't matter how big crypto is in its total value, i.e., if it is currently popular or at a low, having received money connected to a crime could get someone into jail. Therefore, being connected to the criminal world or events via any form of data traces is dangerous and not advisable, at least as long as Cybercrime 2.0 tools are not directly helping them.

(3) Manipulating Law Enforcement

Being caught by law enforcement is an enduring risk of being a criminal. If someone lives in a modern industrialized country while committing crimes, it is only a matter of time before they are caught. Criminals are aware of this risk.

For cybercriminals, it is important not to leave data traces that could be used to connect them to a certain crime or have money or transactions that could be connected to them. Leaving no data traces is no small task. So getting caught as a cybercriminal right now should not come as a surprise.

With more tools and some collaboration among hacker groups, its members will, over time, accumulate enough skills and knowledge, allowing more hackers to stay under the radar and not be arrested until more and better tools protect them individually. This argument refers to an open-source approach to hackers' situations or exposure than doing steps toward a technical solution by themselves. Currently, many cybercriminals are isolated from each other (for their anonymity and protection); they are not well-funded Hackers, so it is unlikely they could develop sophisticated products and come up with Hacker-AI or Cybercrime 2.0 tools all by themselves.

Cybercrime 2.0 will come with Hacker-AI tools, like a "Cyber Trace Remover", that systematically reveal who generates data traces, where they are stored, and how they could be avoided and removed automatically. This tool will reveal enough information to turn it into a “Cyber Blamer” simultaneously, i.e., a tool that could misdirect even digital forensics so that they are made to believe they found the culprit. Hackers’ solutions are based on knowledge, detection of defenders’ countermeasures, and automation. This is an arms race against cyberdefenders, and well-sourced and funded groups could likely win because defenders are currently too slow in distributing their countermeasures.

Law enforcement and courts are handling most cases on and with paper. But these files must be archived or stored as evidence at some time. How and where this storage is done is a secret; even regular police officers may not know the details. Hacker-AI can be used to explore all details. It is unlikely that location and procedures remain hidden from attackers. Much of the standard information is scanned and stored electronically. Changing information requires paper forms that must be filed correctly, but if they are missing, then this is what happens when humans make mistakes. So an electronic record with a scanned paper document is better than nothing - but these files are all vulnerable; it’s just a matter of time.

Additionally, if the software attacking the judiciary with Hacker-AI finds out more about the clerks responsible for the evidence and how they are handling evidence, then Cybercrime 2.0 could start attacking the evidence that is being used against them in criminal investigations and court hearings. Without the physical and irrefutable evidence of a crime, people will presumingly not be convicted due to hearsay or vague memories. Once files on the evidence or the evidence itself are gone, the case is over.

There is redundancy within the judiciary system, but with the right insiders, each system can be compromised covertly, in particular, with in-depth surveillance from smartphones. As assumed in Cyberwar 2.0, most people could be intimidated or bribed and turned into compromised insiders. These insiders could even be instructed to provide misdirection to blame others. However, could monitored suspects, i.e., officials suspected of being bribed, receive money inconspicuously? Well, the right answer is probably: we will see. For leaving no evidence for these crimes, it is important that Cybercrime 2.0 bots or tools are not getting sloppy in these later stages.

Manipulating, compromising, or destroying evidence in court/legal cases could become the ultimate Cyber Jailbreak service that could be provided by Cybercrime 2.0. Independent investigations are certainly opened so that the organizational hierarchy receives answers on how each event was done. But then, who wants to put himself in the line of fire or enter hell of being spied on by malware and/or harassed by automated bots? These investigations are likely closed based on misdirecting evidence conveniently presented to these investigators so they can quickly close the books on it.

Hacker-AI used in Cybercrime 2.0 doesn’t need to meet high standards of secrecy or undetectability when applied against regular, unsophisticated adversaries with average computer skills. Malware from cybercriminals does not need to be hidden like cyberwar weapons - cybercriminal tools can show themselves to people without ringing war bells.

Remain hidden and having methods to protect their main business assets (i.e., malware that facilitate these jailbreaks) is essential. Investing in additional resources and features for staying covert within investigations is helping these hackers and cybercriminals to persevere with their existing tools in business longer.

Existing security tool manufacturers will try to detect these advanced malware tools, particularly on smartphones. Still, they failed with Pegasus, and there is no reason to assume that new tools are not significantly better 8 or 9 years after Pegasus was launched.

(4) On- / Offline Identity Management

Many criminals must hide and adopt a new identity. However, living with a fake identity is risky, expensive, and inconvenient when done unprofessionally. Digital traces make it easier for law enforcement to track people hiding underground.

Even cybercriminals working from home could face the risk of being found out as suspicious developers collaborating on criminal IT projects. Some “metadata” could raise alarm bells with security services and agencies. Cybercriminals know this, which could motivate them to provide these services and get anonymity beyond proxy-server or TOR (short for “The Onion Routing” project) in their offline existence.

Creating believable resumes with fake items could quickly reveal problems in someone’s past when these fake items are questioned. Blending in new environments could require that, e.g., letters of recommendation or testimonials must be faked convincingly. Cybercrime 2.0 tools will be able to counterfeit the certifications of public notaries. Fabricated documents increase the credibility that must be delivered and established before becoming a fully accepted member of a new community. This tool, i.e., a Resume Builder, could use Hacker-AI to create all required info on other systems so that someone’s vita could be checked via the corresponding electronic records without creating suspicion. No one is checking paper archives anymore, except investigators going deep on applicants filing for a top security clearance level. If records are scanned, like yearbooks or facebooks from graduating classes, then names or even pictures could be manipulated by tools controlled by malware and the resume creator. I believe even a social media history could be faked, generated automatically, using AI tools producing the textual content and fake images.

Higher positions raise less suspicion as they require more effort for validation to get into them. Often, these positions require personal testimonials through phone interviews. AI has already shown that it can sufficiently impersonate a person in limited contexts. It is already possible to deep-fake credential checking in phone calls and soon in video calls.

Using malware from Hacker-AI to keep a person undetected is something that some people find very appealing because detection could endanger their life or get them in prison. Making someone vanish and untraceable, blending into a new community is done by governments within witness protection programs.

For cybercriminals to become legitimate business people with a clean past helps them to travel the world safely even if their original name is listed on sanctions or even the most wanted lists. Governments are using bio-identifier before letting people into their country. The Resume Builder should also be capable of preparing Border Control and Visa Management Systems. Cybercrime 2.0 in managing and protecting identities should not surprise.

(5) Cyberwar 2.0 as a Service

Many successful entrepreneurs were refugees. They needed to leave their country when they were teens or young professionals. Some successful people left their country for political reasons. There are no statistics on how many filthy rich people live outside their homeland as ex-pats in other countries with ill will toward the government of their previous home. Many countries with centralized political systems could be in danger if there are services that would help potentially disgruntled retirees to change the regime in their home country.

I have seen many people, and once I met someone who could fit that profile, passionately talking about what they have lost in their homeland. This sense of belonging to their previous homeland is likely being handed down to the next generation. Changing the political and economic system could give some of these rich entrepreneurs a newfound purpose to do something historic for their people. So, a market is likely available for this product or service.

I can understand people with these motivations, but I can also see more nefarious usage of these offerings that criminal organizations could set into motion. We already saw private militia groups in Russia (Wagner-Group), Afghanistan, or African countries that fight wars for their private business. The drivers for these wars are not nations or states trying to pursue political goals, but these conflicts are profit-driven by the warlord's agenda to continue the war as a source of his power and influence. The same would be a "regime change as a service" business provided by Cybercrime 2.0.

The risk is that governments could be overthrown, and in its extension, these private services could commercially exploit these countries in the follow-up. These criminal groups would be legitimized, and their money laundry would be simplified as part of the business deal. Additionally, there is no guarantee or reason to assume that the new rulers care about their fellow citizens.

The new government may establish itself with a new authoritarian leader or even create an AI-based surveillance system to suppress dissent; they could be as bad or worse than the old one. It is too dangerous to let money alone paid to mercenaries decide what happens to a country and its inhabitants. Cyberwar 2.0 should not become a commercial or criminal business service.