7. Cyberwar 2.0 - A New Frontier in Warfare

Cyberwar 2.0 - Phases

Cyberwar 2.0 is the next generation of cyberwarfare, using malware-generating Hacker-AI. It represents an evolution of warfare where cyberattacks are not just about stealing data, espionage, or widespread destruction or disruption. The main focus of Cyberwar 2.0 is to overthrow governments. This new era in warfare poses a significant threat to national security.

On a high-level view, every Cyberwar 2.0 is deniable. When it happens, Cyberwar 2.0 will be very hard to detect and even harder to prove. I hypothesize that the next step after replacing the government is establishing an AI-based surveillance system to secure the spoil of war.

This cyberwar will be fought in several phases, which show different characteristics and could be detected with different tools. War operations are organized in three distinct Cyberwar Phases (CWP-1): pre-war or preparation, (CWP-II) actual war, and (CWP-III) post-war or aftermath. Different activities and goals define them. Probably only the second phase can be called an act of war.

CWP-I (Pre-War or Preparation)

The targeted and soon-to-be-attacked country is being surveilled intensely and covertly, primarily via its citizens' smartphones and computers. This will create a comprehensive data model of its leaders, businesses, and citizens, including their motivations, assumed pressure points, vulnerabilities, strengths/skills, security, and processes. Additional reconnaissance will generate a model for resources, geography, infrastructure, available computers/smartphones/software or hardware, etc. These models will allow the assailant to simulate realistic Cyberwar 2.0 scenarios and post-war challenges. This can help him prepare his resources and optimize his automated attack plan, which I have called war script.

From this model/simulation, the assailant derives a comprehensive, detailed action plan to replace the existing government with a new puppet regime, including actions to make the new government operational by effectively taking full control, including who will be promoted, who will be demoted, or even arrested.

The war script related to malware will automatically determine when and what is being done under which contingencies to reduce possible damages and costs. The war scripts are designed to automate all cyberattacks, including rules for unexpected eventualities or irregularities.

The war scripts are the foundation of Cyberwar 2.0. In exercises and simulations, they are applied to the surveillance data and continuously optimized based on expected but random variations in the feedback given by the targeted country. Some aspects of war scripts might be tested in the field to see if they are sufficiently comprehensive or accurate.

Detailed intelligence is likely gathered on the soon-to-be-attacked country's future (business) vulnerabilities. Simulations will reveal what specific espionage and measures toward lowering the pain from sanctions will be required. However, CWP-I would give only additional urgency and focus to what is already being done.

Because of the almost ghost-like features of the used malware/spyware or the piggybacking on misused commercial software products or their updates within the Cyber Reconnaissance, surveillance operations are expected to happen undetected, or they are being attributed to patsies.

CWP-I ends if assailant's leadership believes that it has sufficient good-enough data for its operation. Simulations would predict a victory as a high-probability outcome. This conclusion could be confirmed via in-detail (realistic/dry-run) simulations. CWP-I surveillance will likely continue in follow-up phases.

CWP-II (Actual War)

No textbook case can help us to define when a (real) cyberwar starts or ends. So far, cyberwar actions have annoyed or scared citizens in targeted counties, or cyberattacks were part of a kinetic/destructive war. No country has been defeated by cyberwar alone. No government has been exchanged as a result of a cyberwar yet. Due to its significant impact on the sovereignty of a nation, Cyberwar 2.0 is correctly called a war.

I define: **Cyberwar 2.0 begins when the assailing country infringes via coordinated cyberattacks on the sovereign rights within the targeted country's territory**. So espionage or putting some malware on users' smartphones or IT devices is below the threshold of war. However, a large-scale Cyber Reconnaissance operation, if detected, should be called an act of war, although it is being considered part of CWP-I. Other examples of acts of war are giving fake orders (on significant activities) by pretending to be a government authority, having citizens arrested (by local police) based on pretenses/fake evidence, or having people (with governmental roles) intimidated/coerced to turn them into traitors.

Additionally, manipulating or having the capabilities to take control over infrastructure services (e.g., power, water, communication/Internet, CCTV surveillance, money supply, financial or eCommerce transactions, logistics, transportation, healthcare, etc.) or security-related resources like command and control of police, military, countries weapons or logistics, etc., could also constitute acts of war.

Assuming the primary goal of Cyberwar 2.0 is the digital decapitation of a country's government and society, every step toward that goal is an act of war. Examples: approaching mid-level clerks, intimidating them to collaborate with the attacker, or selective disruption of communication of higher-level institutions or leaders must be considered acts of war. Deep-faked orders issued to key people in security could make them unwilling collaborators in arresting leaders, influencers, or security people under pretenses. The military could also be ordered to stand down or be isolated from what is happening. All these types of cyberactions could (likely) be considered acts of war because they could be part of replacing the existing government, and they have no other alternative / criminal justification.

As part of misdirection, cybercriminals could be given cyber-tools to create confusion and diversion. The assailant could encourage them to commit more cybercrime events. The assailant could try to distract with news and social media or intimidate or order media outlets to report normalcy. The use of social media could be sabotaged by malware for people known to send out political or critical content. Social media bloggers / influencers could be intimidated to delete or retract / correct their posts.

Justifying a coup or government exchange would probably require some political theater, fabricated disasters, or serious tensions among the political class. This theater could be delivered in various forms depending on circumstances or opportunities.

Many governments have arch-rivals, filthy rich entrepreneurs who were ousted for political reasons and may do anything to return to their country as a savior. These groups could be accused of buying their way into the new leadership. It is also conceivable that a physical (violent) escalation within the inner circle or security forces is turned into an assassination, in which, e.g., people were coerced to smuggle in and deploy explosives to eliminate government's leadership.

Cyberwar 2.0 ends with establishing a new puppet government controlled by the assailant. This new leadership will probably replace the previous bureaucratic and security leadership with intimidated (lower-ranked) collaborators from the target population. Additionally, members of the previous security services are either dispersed or arrested.

To achieve this outcome, no (foreign) soldiers have to enter the targeted country before being officially invited. A new government's legitimacy is often difficult to determine from the outside. Foreign countries must accept nations' sovereign decisions if no proof of foreign interventions or involvement can be provided. Therefore, the only reasonable action the old government could take is to declare the “Country is Under Cyber-Attack” - a declaration that I abbreviate with CUCA and discuss below.

CWP-III (Post-War or Aftermath)

After the cyberattacks result in the expected outcome, it is important for the assailant to fortify gains and to make all change permanent, i.e., irreversible. In this phase, the surveillance is continued. Suspected resistance fighters or saboteurs will likely be arrested and placed in, e.g., reeducation camps. Still, the biggest impact of Cyberwar 2.0 is on the people in the attacked country; their freedom is taken permanently.

This phase aims to reduce possible damages from sanctions that could affect business continuity and reduce the value of the spoil of war. However, if there is no violence, and the puppet government is seemingly accepted by its citizens, the large-scale use of reeducation camps could potentially be postponed, primarily because surveillance from CWP-I is still active and focused on securing public safety while criminalizing any individual resistance act.

Misdirection and propaganda are used to shift the blame to others. Fake news creates a narrative that helps to calm down possible shockwaves and panic reactions worldwide.

Without being prepared for Cyberwar 2.0, it is unlikely that the attacked (old) government could send a CUCA signal (justified by evidence) in which they trigger prepared emergency regulations for the continuation of their government. More importantly, this CUCA signal could affect other countries, as discussed later.

If a country was overtaken (almost) overnight with a cyberattack, everyone involved in national security would ask, how can any country, including the USA or alliances of nations, protect their sovereignty? Therefore, deniability and misdirection are essential to avoid direct retaliation or sanctions.

But without other countries beefing up their security against Cyberwar 2.0, they will know that it is just a matter of time until they are next.

Comparing Cost of War: Conventional vs. Cyberwar 2.0

Military planners focus on destruction rather than the covert utilization of adversarial resources. Defenders often argue that resources should be destroyed before they are in the hand of the enemy. Destroying capabilities give defenders no time to prevent or mitigate damage - it is also irreversible. The question of who is calling for the destruction is a matter of who sees an advantage. The core idea behind Cyberwar 2.0 is that attackers destroy nothing - only deactivate temporarily.

Besides the loss of life, destruction creates sustainable disruption and high costs of loss, replacement, or extended time for repair. Conventional wars are extremely expensive. Still, attackers and prospective winners grudgingly accept that they are in charge of dealing with the damages after winning. If they only exploit the resources of the occupied country, then the new territory remains likely a source of unrest. The losing/victim side suffering from (permanent/physical) damages by the assailant is often reinforced in their resolve to continue their fight. It's much better for both sides if economic resources/ capabilities are not destroyed permanently.

Destruction is based on a fire-and-forget mentality; it is a synonym for war. Cyberwar 2.0 could change that thinking. A modern country is defeated once its regime and bureaucratic/security-related leadership are replaced.

Pre-cyberwar, invisible (software) failures have different effects. In peacetime, coincidence, crime, or incompetence/greed of operators could be blamed for service outages. Software problems don't sound permanent. We could have the hope, even justified expectation, that things can be quickly fixed (why not use backups), triggering often unrealistic expectations of what happens within a cyberwar. However, backups have the same problem - a fix requires an in-depth understanding of the attack. Still, disinformation or active suppression of more accurate news during cyberwar could support attackers' interests and narratives.

Framing it in an analogy: malware is more like human injuries that require continuous attention; it is like anti-personal mines directed to create extended havoc or significant inconveniences around injured persons or within their surroundings than creating death or irreparable (material/permanent) destruction. However, with malware, painful inconveniences can be switched off by the attacker, and a back to normal is possible instantaneously without permanent damage.

In the big picture, today's war costs much more than the attrition of weapons and direct damages from destruction. People are dying, fleeing to other countries, and contributing to other economies. Also, sanctions are imposed, designed to punish the aggressor's economy and the life quality of aggressor's citizens. Once implemented, sanctions are enforced for the long term, and circumventing them is expensive.

However, predicting and preparing for business disruption from sanctions is much cheaper and less painful than suffering unprepared. Improving data transparency on (real) current/future economic vulnerabilities could mitigate aggressors' concerns about uncertainties or surprises from unknown consequences. Cyber Reconnaissance, i.e., systematic espionage on suppliers (in sectors with uncertain/risky dependencies), could reduce the transition time to greater independence, thereby lessening deterrence from third-party sanctions. However, automated reconnaissance on possible business bottlenecks would likely require an AI to extract operationally useful data; if this is already doable (in 2023) is unknown. If commerce (particularly in manufacturing) is not disrupted in the occupied country, global markets are less encouraged to seek replacements or create opportunities for new but unproven suppliers or manufacturers. This argument is important, e.g., with Taiwan and its microchip/-controller manufacturing business.

The advantage of haven a less costly and damaging war is that, at the same time, the main problem with Cyberwar 2.0: it significantly decreases the cost of war for attackers, and it has a high net-positive outcome predictably. Waging cyberwar becomes good business and is, therefore, much more likely. Threats with sanctions would only accelerate deglobalization. Hacker-AI-based spy-effort before and during sanctions motivate corporations to manufacture where they sell and depend less on long/global supply chains. The reduction in destruction/sabotage that significantly reduces the disadvantageous consequences of wars would simultaneously increase distrust between countries.

Where could Cyberwar 2.0 Happen?

Many countries have the technical prerequisites to develop and political motivation to use Cyberwar 2.0. I will discuss two countries with applicable scenarios. And I will discuss a rogue scenario in which a criminal non-state actor is pursuing Hacker-AI and what that scenario could look like.

USA Using It Against …

The US is probably the country that could develop Hacker-AI immediately or has large parts of it already developed. It is not assumed that the US government has the programming capacity/skills to do these tasks. It has also enough math expertise within the NSA (National Security Agency) alone to work out easily the algorithms required for the various optimizations and data aggregations assumed to be used in Cyberwar 2.0.

It is also conceivable that the US government uses knowledge from US-based top-notch low-level system developers and AI researchers to get the required frameworks for the tech library and tech simulator pushed forward quickly. The US may use additional spyware expertise from Israel, mainly from the (previous) NSO Group, which may contribute to Cyber Beachheads, Cyber Cradles, and Cyber Whispering; however, when done, Hacker-AI may deliver next-generation solutions surpassing human experience. Related to the AI used for hacking, it seems that the required knowledge on several approaches to this task is widely available. So recruiting these experts in special teams within the US is doable. With DARPA (Defense Advanced Research Projects Agency), the US has the project management capacity to complete the required technology quickly.

So then the question is, where could the US use Cyberwar 2.0 first? In 2023, the USA has four major adversaries: Russia, China, Iran, and North Korea. Iran and, more so, North Korea will be discussed in a Cyberwar 3.0 scenario, in which not just the government would be replaced; more importantly, military equipment, i.e., the large arsenal of weapons, would need to be predictably neutralized/sabotaged. China represents a danger to Taiwan and potentially to the entire world if China controls Taiwan's semiconductor manufacturing capacity. However, it is assumed that the USA has no appetite to start a war or cyberwar with China in the next few years or decades. China is considered a valuable trading partner, a global competitor, and not an enemy.

I am left with Russia, a country that started a war of aggression with Ukraine. When this book was written, Russia seemed to be on the path of losing this conflict. I am not a prophet or political forecaster on how this conflict could evolve/end or an expert on how Russia could spiral down further. Also, I don't want to suggest how this conflict could be resolved with the US getting more involved. Still, with these disclaimers, I am an observer and have an opinion.

It seems the US and most NATO countries worry about what happens when Kremlin's political leadership is further cornered. Security experts are likely brainstorming how Russia could be put on a more peaceful path to a sustainable future. The most important problem is Russia's large nuclear arsenal that it could use to defend its national integrity and sovereignty, i.e., if the state's existence is being threatened.

Based on the deterrence from the nuclear arsenal, it is unlikely that the US will proactively start any steps to trigger a regime change in Russia. It would only do that if it had solid cyber capabilities that could (temporarily) knock out or freeze the command and control system until a new government in Russia/Kremlin is fully established. A freeze would mean that the nuclear arsenal is completely neutralized.

Some scholars like the political scientist Alexander Motyl and activist/journalist Sergej Sumlenny assume that Russia could fall apart. Sumlenny sees Russia collapse into a conglomerate of different ethnic republics or provinces seeking independence from Moscow while unilaterally taking control over territories and resources. They may separate themselves from the central control in Russia for various economic reasons. Russia has 46 oblasts, which are administrative divisions or regions of Russia; some could strive for independence.

Russia is under heavy sanctions by the world community. It has a high-tech infrastructure with smartphones in the hand of almost every person. Many tech-savvy people and filthy rich oligarchs are unsatisfied with the country's trajectory. On the other side, it must be assumed that the Russian security services use high-tech measures to detect dissent/protest and prosecute opposition to the current regime to a cruel level. Most oligarchs, even those living outside Russia, are likely under surveillance. Getting in touch with people who could make a difference is dangerous for them and their families.

If the US decides to use Cyberwar 2.0 to change the regime in Russia, then they would probably enable Russian oligarchs and dissidents to coordinate and organize themselves more closely and covertly. The US could enable the opposition and separatists among them with intelligence that effectively destabilize the system even further. Oligarchs, who want to return to their previous global lifestyle, could be supported to exercise their moderate influence and stop radicals or extremists from misusing this trend.

Russia has 145 million inhabitants, 81% are ethnic Russians, and 75% live in or close to urban centers. About 85% are part of the European Russia territory (i.e., west of the Ural Mountains), and it is estimated that one to three million are somewhat relevant (1-2%) for the success of a coup carried by the populace. But really relevant are only a few ten-thousands among them who stop distributing or actively sabotaging orders. Additionally, an estimated 5-20% could become relevant due to their expertise, education, or position within Russian society for restarting the society and its economy.

Getting possible key players identified, organized, and their actions coordinated is difficult as the Kremlin has an iron grip on mass media, relevant parts of the Internet / social media, and the legal / security apparatus. The Russian government efficiently gets people arrested who threaten the political establishment.

With Cyber Reconnaissance and stealthy but activatable malware on millions of relevant smartphones or computers, the Russian opposition could get governmental control over several oblasts by direct access to essential parts of the bureaucracy. The opposition could use reliable and immediately useful intelligence as currency to protect the security and well-being of officials and their families.

It is conceivable that the legal system, security services, and nuclear forces can be sabotaged by malware, potentially by people working in these sectors. They would do this out of concern for what could happen to them or their families if their situation goes from bad to worse. Although many of them are under surveillance, Hacker-AI could find ways to bypass standard (digital) surveillance and help to connect with these people, potentially via their families. The US has probably enough records to connect the dots and determine who could be turned into collaboration over time or who is a hardliner. It is not required to go directly after everyone who is considered relevant; instead, it is better to leverage the potential of a few to get specific missions done at the right time and location.

The money of oligarchs and their contacts in critical private sector activities could be very important to stabilize the economy after the collapse of the old regime. With AI and ubiquitous smartphones, it is conceivable to build a small business economy efficiently fast; some ideas are shared in Cyberwar 3.0 (aftermath). Providing targeted information to 145 million Russians in the aftermath could mitigate humanitarian and social problems from disruptions in the political arena. Large parts of the police force could be trained and used via (concrete) instructions sent via the Internet to their smartphone to take charge of public safety beyond crowd control and crime-fighting tasks. Supplying these tools/hardware and providing the software is part of the contingency/preparedness planning required for these scenarios.

The Kremlin has created a bubble around Putin for his security and command and control over the security and nuclear forces. Understanding this bubble will reveal weaknesses, particularly from a lack of motivation or desperation. It is not the goal of Cyberwar 2.0 to facilitate the assassination of political leaders but to isolate them enough to make it easy for the opposition to replace identified key positions in the chain of command with people that administer their organizations. They will not listen to the Kremlin or people who operate on Kremlin's demands if that is detrimental to their interest. Once people see that defiance does not lead to consequences, they may join quickly.

In reducing the friction in the transition to the new leadership, it could be suggested that the old regime should be given a "golden bridge" to save their lives. This bridge could be done by assurances communicated to close leadership advisers on how the escape could operationally be guaranteed.

Even without coordination, authoritarian regimes usually fall apart rapidly, or protests turn violent, with police/security forces inciting it. With support from the outside, deep-fakes can be used to have security forces stand down so the likelihood of violent suppression of disobedience could be reduced. If a similar influence can be exercised on the chain of command for nuclear weapons is unknown. However, it is assumed that US intelligence is capable of coming up with redundant plans to use cyberweapons and the use of new and spontaneously recruited human assets to mitigate the potential danger of nuclear weapons. In Cyberwar 3.0, ideas on sabotaging weapon systems of all kinds are discussed in more detail.

China is Using It Against Taiwan

The annexation of Taiwan, or the Republic of China (ROC), is the declared goal of China, or more precisely, the People's Republic of China (PRC). China has technical cyber capabilities and strong motivations to occupy Taiwan; they are even willing to accept the extreme risks of a costly conventional war to accomplish this goal.

Because of China's urgency to take over Taiwan, it is conceivable that Taiwan could become the world's first example of Cyberwar 2.0. Because of PRC's political priority for ROC, they could attack ROC as soon as they have an early version, potentially a less scrutinized version of Hacker-AI and tools supporting Cyberwar 2.0. The operators may not be fully convinced that the produced malware is as stealthy as it can be or certain surveillance features are more labor-intensive. Still, China could start a Cyberwar 2.0 attack without declaring war while trying to deny any hostile involvement. China may play for additional time to improve its tools or avoid a global escalation. With less stealthiness, they could potentially blame a wealthy inner-Taiwanese opposition that disagrees with the current government on how to defend Taiwan.

With the availability of many public records, Cyber Reconnaissance would be easier and faster to get focused on the relevant people who could play a more important role in a government overthrow. It must be assumed that the PRC has enough intelligence about ROC to create a playbook on how Taiwan's governments could be destabilized and then replaced by a new group of politicians that have been intimidated or bribed to become an interims solution until they prepare steps that would put Taiwan on an irreversible course to its annexation.

Without showing any obvious signs of imminent collapse, ROC's sovereignty could end effectively after some decisive covert cyberwar steps digitally decapitate the government and society. Most citizens or news media would be oblivious to what happened. Some people in the administration's middle or even lower tier would be intimidated into being (silent) collaborators.

Collaborators (and internal enemies of the existing order) are identified; they could silently take over operational key positions via faked orders, while higher echelons of the government are technically incapacitated and silenced. Also, some cyberactions are likely to distract from more essential policy changes and the use of CCTV cameras for surveillance (instead of public safety).

The Taiwanese military doesn't have anyone to fight except a new government that legitimacy it may not accept, an attitude that may not be shared in all parts of the army. Also, China/PRC may not have sophisticated malware that could (temporarily) sabotage or deactivate (software-based) military weapons. China, with its Hacker-AI, will likely have the ability to disrupt the logistics of ammunition, i.e., shipped to locations where it can't be used by troops loyal to the old government. Instead, logistics would exclusively favor the troops loyal to the new regime so that they could use them.

Finally, some business consultants (operated by PRC intelligence services) are invited as "experts" to reinforce (legal/ technical) ties to PRC. The new government is not expected to set constraints on AI-based public surveillance. Due to ROC's (cyber-) decapitation, USA's influences within Taiwan will cool down until it is quickly neutralized.

Over the next days and weeks, the USA will realize that it has no legal basis to be involved in ROC's internal affairs, certainly not militarily. Deterring PRC would require ROC to destroy its own country (via sabotage) to increase PRC's costs of waging this cyberwar. However, sabotage can be suppressed by mass arrests and large reeducation camps for people accused of dissent (like the Uyghurs).

As a result of this event, the USA may reinforce its 2018 nuclear posture, which includes cyberattacks as events in which they might respond nuclear. However, Cyberwar 2.0 activities changing foreign regimes covertly are probably below the threshold of nuclear retaliation. The problem is that Hacker-AI capabilities are difficult to determine and detect. Additionally, its scale of deployment is unknown until it is (potentially) too late. Unfortunately, retaliation capabilities might be affected or even effectively sabotaged and neutralized already, which is extremely difficult to determine. The speed of a cyberwar attack may not give targeted countries any option to respond. The full penetration of all IT devices with Hacker-AI generated-malware, i.e., from establishing all Cyber Beachheads to almost irremovable Cyber Cradles, could take 3 minutes or 3 seconds - nobody can know today.

A successful Cyberwar 2.0 on Taiwan would probably send shockwaves through the world. If ROC could be overtaken, how can the USA or some other nations protect their sovereignty? At that point, deniability and misdirection are essential. Without proof, an uncontrolled, fear-triggered escalation close to nuclear war is conceivable. However, nuclear retaliation without proof seems unlikely. Instead, we should hope that a massive mobilization of technical talents is initiated. How fast or successfully we can react depends on many unknowns. The problem is that it might be too late.

Rogue Actors Providing "Regime-Change as a Service"

With technical progress simplifying the development/deployment of surveillance capabilities, building offensive Cyberwar 2.0 capabilities becomes easier by the month. There are many highly skilled developers and technology designers with an understanding of what needs to be accomplished by Hacker-AI and its corresponding features. This book has elaborated on many details, but this is nothing that a smart senior developer or CTO (Chief Technology Officer) would not come up with by thinking about this for some time or discussing it with a team of A-players.

The question is only speed. How long would it take to get to a level of excellence so that the government's leadership would put their destiny on the success of this tool?

Others would use their money for expedited development. They would not be too concerned about stealthiness as they don't care about long-term political consequences or their historical legacy. I am talking about more criminal-minded entrepreneurs who see their advantages in providing a solution for governments that don't have the technical expertise in their country. Also, super-rich ex-pats, ousted from their home country, are impatiently pushing to return. They want to be either their homeland's new political leader or a retiree who sees himself as the savior of their country from evil wrongdoers.

Most countries are vulnerable to coordinated cyberwar attacks, even in developing countries, because smartphones are already omnipresent. Additionally, countries "liberated" by Cyberwar 2.0 could probably be considered safe havens for everyone involved in providing the Hacker-AI and Cyberwar 2.0 features and for others who want to use Hacker-AI in Cybercrime 2.0 applications, as suggested n the next chapter.

The NSO-Group has provided a business model for its Pegasus software in which it helped nations and their governments, including law enforcement or intelligence services. They were deliberately not serving their opposition. If criminals would redo the Pegasus features using AI to accelerate the hacking, then this group or these groups would probably need to find places in which the developers are safe during the development from being harassed by local law enforcement or intelligence services as it happens in Russia currently. More important, they must be safe from the wrath of the long arm of the US government. I will not make suggestions, but I assume this is feasible to work for a while under increased security constraints in countries with less than first-world public amenities or freedom of expression.

It is possible for a distributed group of professional hackers, system developers, and AI engineers to use additional competencies for which they hire expert freelancers to develop in secrecy tools that much larger nation-states or military superpowers are expected to develop. Money spent by a smart CTO, who knows what he wants, could delegate the required component development. Most of these components are high-level and would not reveal the final use. Other components could be motivated by cover stories that developers could believe and not think further about if the money would be ok.

These rogue developers would seek protection and, if they are smart, a way to retire with generational wealth that they got laundered by tools supported by Hacker-AI. So finding countries where they could become ordinary citizens would be one goal. Risking their newfound home or community by collaborating with dangerous criminal organizations and terrorists might be initially outside their comfort zone as they would live in the same dystopian world as everyone else. Providing Hacker-AI for extremely damaging use might be a matter of having some leverage against international law enforcement.

Although some Hacker-AI technology might be developed independently anyway, it is conceivable that code of some core-Hacker-AI features is being put in a data/software vault that is being opened automatically if certain hackers fail to insert their key in regularly. This system, also called a dead-men-switch, could be designed by criminal developers to blackmail governments into releasing them, or their code would be published under the freedom of speech. The code would enable other less brilliant software engineers to shortcut their development time to create nefarious Cybercrime 2.0 features. It would allow many more groups to automatically release their Hacker-AI that generates malware for all OS platforms. At that point, malware capable of stealing crypto-keys would soon get into the hands of international criminals or terrorists that could undermine the trust in eCommerce or online banking.