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

8. How is it to be in a Cyberwar 2.0

Many people have gone through the horrors of conventional war throughout history. Soldiers, civilians, and children have all been affected by war's violence, destruction, and trauma. People endured unimaginable conditions, such as bombings, gunfire, and the loss of loved ones. They faced war's physical and emotional effects: injuries, displacement, and post-traumatic stress disorder (PTSD).

War survivors must adapt to new realities marked by physical and emotional scars, economic insecurity, and social upheaval. They must rebuild their lives and communities, often with limited resources and ongoing violence, poverty, and political instability. Children are particularly vulnerable during a war. They are often forced to flee their homes, lose their families, and face the trauma of violence. The trauma, the memories, and the long-term effects continue to shape people's lives long after the fighting has stopped.

Comparing the horrors of war with Cyberwar 2.0 is obscene, like comparing the death of a loved one with an insult. Still, cyberwar can tear apart the fabric of societies, erode trust and security, replace the government and establish surveillance that could last for a long time.

Cyberwar 2.0 is not an event that will be acknowledged by the party using it to attack another country and its government. The attacked government could, e.g., claim that the coup had foreign involvement and was cyber-based. But these words and claims are cheap. It's likely impossible to substantiate this claim because there will be no hard evidence, only speculation. I will later discuss how countries could still prepare for this situation (see last chapter) and announce that their country is under cyber-attack (CUCA) - but that won't change the outcome: there will be a new regime, a new government. It will change people's lives and their freedom significantly.

Cyberwar 2.0 will probably play out in the shadows and entirely undetected by the public until it is too late. In the following section, I want to give an impression of how different perspectives and actors will perceive the events around Cyberwar 2.0. I am starting with the (a) public view. Then, (b) is about people like clerks or officials who are intimidated - it will describe how it is on the front line. Others will become unwilling tools like (c) security officers. The government (d) may receive information and carefully document events leading to the coup while the military expects an invasion. Finally, I want to include also the perspective of the (e) assailant, how they are preparing, training, and executing cyberwar scripts.

Public View

So how would a Cyberwar be perceived by the public, most of the government, and even by the mass media (press, TV)? In short, nothing is happening until, suddenly, news prepares the public that some crisis or scandal is being discussed within the top echelons of the government.

All this is speculation, but it is an example showing that these scenarios are not far-fetched.

Mostly rumors designed by experts for propaganda or psychological warfare (PsyOps) will influence the population's attitudes toward a more favorable environment for a (desired) change. Some messages will undermine the existing regime's legitimacy and promote the benefits of a new regime or create scandals that involve manipulating people's emotions or perceptions of the existing government. Only voices calling for a clear break from the past and a new beginning are being published. Even opinions known to be cautious or opposing radical changes articulate their hope that things are no longer stopped or that "Golden Offers" or compromises provided by someone are not being dismissed.

There will be some manufactured urgency, something that must be accepted soon, or this opportunity is gone. The deal is praised as a long-expected breakthrough and demonized as a poison pill or capitulation by the government. Even government's defenders will be heard in public, but their opinions are toned down, apologetic in defense of the old government. The government presents itself as a reckless hardliner. Because of malware-based media control, nothing must be true here; all is theater. Some journalists may have phone or video calls, but they are deep-fakes, and the reporters have no way to validate them.

At some point, the old government got quiet; until a TV recording of the head of state declaring that it had resigned and had transferred the power to a new government or head of state. This recording could also be deep-faked, but this possibility is being dismissed by the top journalist, who might also be deep-faked or intimidated to stick with the provided script. The entire event might be presented as life, but it will likely be delayed by minutes or hours so that external control could step in with on-the-fly generated deep-fakes anytime.

Intimidated Clerks and Officials

The participation and active collaboration of specifically identified clerks, officials, and officers are required to make assailant's plan work. In Cyberwar 2.0, attackers need to turn willing or unwilling helpers against their current government; these people and their choices are the front line. Their actions will make the attacker's war plan successful or a failure. It may not be transparent that they will play an active role in a coup initiated by a foreign power wages Cyberwar 2.0 against their homeland. Most are being deceived. Even if they are

suspicious or trained to resist, they will be massively intimidated because they are part of war actions. They all must obey orders or face consequences immediately or later.

I continue with some speculation. The following scenes exemplify how this could play out.

In Columbia, a phrase was used by drug traffickers: "plomo o plata" (lead or silver), giving a choice between a bad one (lead), indicating a bullet, and a good one (silver) - receiving some gift. If an assailant needs something and considers himself in a war, then deadly threats must be taken seriously. Before attacker's software, a bot, contacts anyone, Cyber Reconnaissance has identified, selected, and narrowed down possible candidates for every anticipated mission. The bot has collected enough information to address their situation individually, personal life, interest, problems, etc. The bot knows potentially as much as the spouse. Once contacted, they are considered recruited and will be called as such. The bot won't ask for further permissions; it's plomo o plata; the recruits need to show from this point on that they are more interested in helping than bots are asking them.

Some people can be impressed by stories of a "powerful group" determined to "rescue the country from turning wrong" or reminded what it could mean financially or for their career goals to be on the right side. At the same time, these recruits are being seriously intimidated, like: "a few people betraying the cause won't change the final result anyway" or "we sacrifice traitors for the greater good - even to make a point that others should see". Bots will show pictures of dead families. The bots expect "orders to be followed" and "nothing is said or hinted to anyone". Also, "we will not forget"; traitors and their families will pay a steep and painful price for "disloyalty".

Later, the bots may say, "we know what you did - why did you do that?" Or "if we are not asking you anymore, then we know something that makes us not trust you anymore", Also: "you and your family will regret that day you did something wrong". Why are these threats so massive? Because it's war, not business. The tables are being turned on them: Recruitees will see and learn quickly that they must please the bots, do something, or worry. They need to accept they have no choice. If the bot doesn't hear the recruitee's desire to please the bot, they may not fear them enough. This is how to live on the new front line.

The bot may even say: "Tell your spouse". Make them part of the commitment. In the expectation that bots could hear into their confidential chats and, from that, determine how they really think over time, the assailant will know if the spouse agrees/disagrees on (not) anonymously reporting their contact to the bot. Additionally, the attacker gets 2 instead of 1 operative.

For covering tracks, the bot may speak another language (like English) with a certain accent, as if the bot is actually a human. The bot could also talk in

perfect or broken Taiwanese mandarin, only to confuse the recruits; it may even say that it is a bot and remind them that technology never forgets details.

Additionally, recruits are tested for their loyalty and reminded if it is worth the risk of being punished for breaking the silence. Anyone knows if they are currently part of a critical mission. Still, tests are about small things, like borrowing a drone, making it available anytime, buying products/stuff online (CCTV/webcams, etc.), and leaving them on their balcony or garden to be picked up by other drones. Or 3D printing parts are produced with recruitee's 3D printer or have them provide 3D model files for their local 3D printing service. Drones will require 1000s of printed custom parts: e.g., to carry a laser pointer, liquid container, etc., to make them more useful for intimidation or operations. These parts are left inconspicuous in different places, accessible for drones only.

Recruits may also be asked to buy (illegal) drugs and leave them somewhere after changing their packaging (with someone else's fingerprints), so others don't see these are drugs. Others will put them in a certain car below the driver's seat after someone else was used to opening the car with a tool 5 minutes before. The attacker may only "borrow" a minute of some recruitee's time who was nearby, or it calls in services to get more difficult things done. 1000s of these kinds of scripts were all tested; no waste because of some missing detail.

Smartphones are used to orchestrate a handover of stuff without seeing who else is involved. What is being done with these inconspicuous items? Is it important for a recruit to report a message to pick up a half-empty bottle of soda, bring it into a secured building, and leave it on the floor beside a vase? A minute later, another recruit receives a message or call to pick it up and put it in his desk. Who knows what that is? Who can put the pieces together and determine who's the target or who was involved? Was it nothing, a decoy, or an incendiary? Is this really worth reporting and taking risks?

Security Officers as Unwilling Tools

Police officers were ordered to arrest several high-ranking military leaders for conspiracy; after a (deep-faked) hidden-camera video recording was provided to prosecutors via a thumb drive - seemingly from some other branch of government. Also, deep-faked recordings indicate that the conspirators were concerned about arrests and that fleeing the country might be the only option. After their arrest, they were released a few days later; they will remain suspended from their duties until the courts decide on the allegations.

For the involved police officers, these arrests were ordered by their higher-ups. If these arrests are justified is not for them to decide. More arrests of security/intelligence service officials and politicians were based on corruption, money laundering, or drug charges. The number of these high-profile cases is surprising. The evidence always seems genuine, bags of cash, drugs under the

driver seat, etc., but they were all fake, planted. The arrests took out people that could potentially prevent a coup, but now, they are fighting false but serious allegations.

These arrested victims are being harassed as if all these accusations are correct; they have lost their reputations and positions. Still, the number of same-day arrests is highly suspicious; the evidence seems irrefutable and ignoring each case seems impossible. The safe option is to wait for the result of more comprehensive investigations - which takes time. But then the coup happened, and most of these high-profile cases were quickly convicted; some got even in show trials, where other charges were used to justify their arrests. These trials show clearly why the old government needed to be replaced.

But the police officer discussed his information about one of these cases casually with his colleague; a smartphone was listening in. In the evening, both got a call, saying something about a report made by the other conversation partner. The message was clear: be quiet or else. Were humans involved in any part of this incident? Maybe, as a supervisor or a trigger-person watching 100s or 1000s of these cover-ups done safely, most operations are automated, chosen from many possible response scenarios, all described in war scripts. Actually, most details can be left to the bots' autonomy.

It sounds like a movie script. Probably, it is. Some people need to think through these contingencies. Why not someone with some movie-goer experience and imagination? This cover-up is (a cheap) part of the warfare. Why create problems with witnesses if the cleanup is so easy?

Governments Receiving Intelligence and Preparing

I assume that a (to-be) attacked country's government has prepared and created procedures for a cyberwar; they hired staff dedicated to cyber-threats. The government's leadership is also aware that Cyberwar 2.0 is trying to change top-government officials. They know that some political theater will escalate and end with a government overthrow. There are no more details. Instead, they aim to detect events where the adversary recruits civilians, clerks, and officials to plant evidence or do something significantly different. They hope that people will report threats or orders that violate their loyalty to the organization they serve.

The next plot could sound like a Tom Clancy story. The government has offices in which reports from all over the country are analyzed. A few reports indicate that adversaries are trying to understand processes within certain administrational sections of the bureaucracy. Unknown callers asked suspicious questions: about how files are handled and who is responsible for certain decisions. These calls and callers were detected. Maybe it was part of a misdirection. From early reports, no clear picture of the assailant's intention could be derived. In one day, the number of reports skyrocketed. But still, all these reports were

mainly about intelligence gathering. There were several days with no reports. Finally, the cyber-threat office could follow up on a few anonymous calls that digital forensics could connect to 2 smartphones. On these phones, they found malware developed by a US spyware manufacturer; data indicated that software was used for the calls; their owners appeared surprised. Additional research in data traces showed data were sent to servers paid indirectly by criminal organizations. Unbeknownst to the investigators, the assailant planted all these findings to blame others.

Suddenly there are other spikes of strange, shadow activities; it looks like someone is planting evidence against military officials, preparing for their arrests. Within a few days, more activities around incriminating evidence, possibly related to security officials or politicians. Then unexpectedly, leaks about scandals, rumors on secret investigations, and their cover-up. Someone went missing; a possible crime scene needs to be checked out.

Some politicians are making suspicious public statements. When contacted by the cyber office, they refuse to answer. Actually, close relatives of these politicians were arrested and then released. They were massively intimidated by their relatives - some of these calls were deep-faked. It seems the lives of their loved ones depend on their silence and compliance.

This plot sounds like a huge effort, but it's not for intelligence operations using Hacker-AI as an interactive tool. A lot of details are coming up within the surveillance. AI is just presenting them and helping to connect some dots; they are then turned into a plan with a few instructions and actions by others. Much of it looks coincidentally. Criminal bureaucrats or politicians got careless and caught in their private scandals. Has Cyberwar 2.0 already started, or is it just related to some Cybercrime 2.0, regular money laundering, or people who got involved with other criminals?

If the cyber office could connect all the dots they receive, would they issue a "country under cyber-attack" (CUCA)? Suspicious events happen all the time, but then no follow-up events, seemingly. Just seeds were planted. Finally, the seriousness of the cyber activities may have been seen too late, and the government tumbled. After that, the new, seemingly legitimate government has no interest in these investigations; they have teams that will deliver their narrative.

Also, the new leadership has seemingly no clear link to the suspected attackers or foreign governments; still, they pursue policies that favor them. Over the next months, large parts of the bureaucracy and the top military leadership are being replaced. The cyber-threat office got new people. Contracts for internal security and CCTV improvements were given to companies with suspicious ties to the assumed assailant. The next election was technically hacked, but internal security didn't find evidence. A few months later, the government started negotiations on association agreements, leading to an official (peaceful) reunification. In the meantime, many people were arrested under suspicious circumstances; some were accused of sabotage.

A modified social scoring and benefit distribution system was introduced in the follow-up to suppress dissent or protest. It seems the country is now a province under AI surveillance. No one could have seen it coming. People seem to be ok with the situation. The economy might be booming, and some say life was never better.

Or will the occupied country face human rights violations, forced labor, displacement, extrajudicial killings, violence, torture, rape, restrictions on freedom of movement, speech, and assembly, psychological trauma, fear, loss of community, and social support? Will children be forced into paramilitary groups and indoctrinated?

The consequences of Cyberwar 2.0 will have a long-lasting, far-reaching impact on future generations.

Assailants Preparing and Executing an Attack

The Cyberwar 2.0 operators are probably high-level officials with mid-level staff that is interfacing with the software and preparing dashboard-type output for the (political) higher-ups. Right after the order for making an "invasion" plan came, goals and timeframes were defined. A small team of planners came to brainstorm and discuss multiple scenarios of how the government overthrow could be accomplished and who precisely could be blamed as possible culprits. Multiple high-level, strategic war scripts were designed.

Additionally, a small city was built, occupied by 1,000s of actors or trained to be actors playing recruits and their families. They were hired to come up with tactical scripts while playing intimidating recruits. 10,000s scripts were designed and field tested under the supervision of 1,000s intelligence and military officials. They were hired to live isolated from their families until some "event" ended victoriously. Most were quite eager to test and improve the bots. No one needs to program these bots; AI in the background learned from feedback - while the actors were supervised. Huge lists of scenarios were created, enacted, and tested. Later, all were released and instructed to keep total silence. Each got a cover story, money for a good living, and an AI on their smartphone listening into their life for an unknown period. If they talk or make hints, they will regret that. They know how good these systems are. No one dares to speak.

After several independent Cyber Reconnaissance campaigns happened over several weeks, the data model for a comprehensive simulation is available for testing the war scripts. The war planners' task is to identify different scenarios while field-testing them in their test city to determine how they perform automatically concerning (potentially) missing follow-up scenarios. The AI in the bots got better, with fewer mistakes; even if they happened, contingencies were designed to keep the interaction with the recruits in flow and focused on the objectives.

The Cyberwar 2.0 simulation mimics all aspects: bots, recruits, events, geography, environment, and even traffic; it's just a large, comprehensive data operation. Also, the feedback systems from the test city are tested comprehensively. There will be little difference between exercises and the real Cyberwar 2.0. For the operators, even leaders following it, it is not a movie; it is just an immersive game with high-level dashboards and higher-ups following the war's progress on TV in parallel.