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

10. Cyberwar 3.0 - Start of a Solution

I should clarify what I mean by 3.0. Cyberwar 3.0 is not the next generation to Cyberwar 2.0. It is a qualitatively new level of waging a (non-lethal, non-destructive) war that requires a different label. It is a war against weapons, not people.

This technology is not about the detrimental use of AI in Hacking, warfare, or crime but a beneficial use in the defense of humans against weapons - a solution against harmful and lethal technologies.

I read a couple of books on the future of warfare. Except for "non-lethal weapons", I never thought their authors gave me an unequivocal attractive vision of our future with weapons, i.e., "yes, this is how our future should be". I don't say that Cyberwar 3.0 is the only new weapon system we will or should have, but it is a weapon system that protects us against other weapons.

Weapons used against other weapons are not new. The iron dome from Israel or the Patriot rocket system is used to shoot down other incoming rockets. Also, primary targets in every warfare are ammunition storage places. So what's new in Cyberwar 3.0 is the use of AI in autonomous weapon systems that are going after other weapons.

I hope this new approach to warfare and defense could become a pattern to solve other problems. In the next chapter, I will discuss solutions to eliminate problems from Hacker-AI, Cyberwar 2.0, and Cybercrime 2.0. Therefore, this chapter starts the solutions section: using outside-the-box ideas to solve our human security problems emerging from the adversarial use of technology.

Cyberwar 3.0 uses drones. From Ukraine, we see how commercial drones, or unmanned aerial vehicles (UAVs), are used in a war against Russian troops occupying their country. They use drones for reconnaissance and for dropping grenades on Russian trenches. We see how Russia has sent drones to destroy Ukrainian infrastructure. We also get news on US kamikaze/SwitchBlade drones or drones from Turkey used against tanks. Using remotely controlled or semi-automated drones or cruise missiles is not new in warfare.

For over 20 years, the US military has used drones to kill terrorists globally from remote places in Nevada or via other remote command posts outside hot battle zones, often thousands of miles from where they are being used. US drones were used in targeted killings; this became increasingly controversial in recent years due to concerns about civilian casualties and the legal and ethical implications of using this technology in warfare.

Drone warfare is defined by using aerial drones for military operations. These drones are armed with missiles, bombs, or grenades and controlled remotely by operators. But they are also used for surveillance and reconnaissance. So when I mention Cyberwar 3.0, I mean autonomous, non-lethal Drone Warfare 2.0 against weapons only.

The idea behind Cyberwar 2.0 and also 3.0 is to avoid any physical damage to property or harm to people. Destruction, disruption, and unnecessary injuries or deaths of people are war costs that the winning party will likely regret that they happened.

According to Sun-Tsu in "The Art of War", the ultimate goal of war is to achieve victory with minimal losses; also: a successful war should be fought with minimal violence, and victory should be achieved by other means than brute force.

What is Cyberwar 3.0

I define Cyberwar 3.0 as a data operation with additional (aerial) drones targeting weapons and people that try to harm others with weapons by using non-lethal violence.

The idea of Cyberwar 3.0 is close to the concept presented in "Slaughterbot", a short video published in November 2017, with the main difference: I propose non-lethal (autonomous) bots. The presented scenario portrayed a near-future situation where large numbers of low-cost microdrones, utilizing artificial intelligence and the ability to recognize faces, target and eliminate political opponents according to predetermined criteria. Microdrones were killing targeted people with explosives. The autonomy of these drones would make Slaughterbots a Weapon of Mass Destruction (WMD).

The group, around the Future of Life Institute (associated with MIT), argued that military superpowers have no interest in dealing with these cheaply produced microdrones. The video portrayed drones as autonomous weapons designed to kill people. However, the purpose of war is not just killing and destroying. This assumption about war is a misconception; using lethal violence is how wars are currently implemented, but it is not the essence of war. Every war has a mission, and killing or the threat with deadly force is only one of many options/methods to enforce occupier's will on the occupants. Actually, killing and spreading terror is a bad strategy; it increases the will to continue the fight.

All weapons have the propensity to be lethal, including autonomous non-lethal drones or stun guns. Terrorists or rogue states can turn DYI drones into deadly weapons. The problem is that we cannot stop the technology that turns ubiquitous consumer drones into autonomous, potentially lethal weapon systems. For defenders, this means (independent of Cyberwar 3.0) we need to focus on defensive measures to counter drones. I will discuss defense measures against drones later.

The most important argument against Cyberwar 2.0 is that many conflict zones lack the necessary infrastructure to conduct a cyberwar. Some leaders in underdeveloped countries may have phones, even smartphones, but lower-level officials or clerks are not expected to have them. Also, North Korea would not have the infrastructure to be vulnerable to Cyberwar 2.0 activities, but it would have the tools to attack us in cyberspace. Also, in civil wars, destruction has already happened.

Cyberwar 3.0 Targets

In short, Cyberwar 3.0 weapon systems target and destroy weapons carried or shown in the open. It will do this with non-lethal but effective means. Special miniaturized Cyberwar 3.0 microdrones will create an environment where handguns can only be carried concealed or by (face-)recognized people authorized to do so. Soon, soldiers and their military equipment are deterred from getting out of their barracks and exercising with their weapons in the open; drones could ambush them.

One of the main targets of these drones is the gun's barrel, i.e., barrels in artillery, cannons, tanks, and later rifles, and even handguns. Barrels are usually made out of metal; that can be affected by certain chemicals or metal pieces that could destroy the bore, i.e., the internal lumen, of a barrel as soon as a shot is fired.

The bore often has helical flutings that can be used within the sabotage via glue, acid, and small triangle-/pyramid-shaped metal spikes that would maximize damage to the bore when it got in touch with a fired bullet. Glue and acid could make it extremely hard to get the bore cleaned. Multiple drone attacks on a single bore could use small bullets or darts (containing the mentioned spike, acid, and glue) shot into the gun's bore, which disintegrates and chemically reacts with the bore. As a result, the barrel is dangerous for the shooter or operator of the weapon; the bullet or grenade could make the barrel/muzzle explode.

The weapon operator, gun user, or shooter could try to protect the bore by putting some cover over the top of the muzzle. However, simple barrel protection is not enough; drones could use fire on other parts of the weapon. The fire could be ignited with a few drops of sticky napalm to vulnerable weapon parts with a laser-triggered igniter. Experts can study each enemy's weapon system in detail for these types of vulnerabilities and catastrophic damage from small acts of sabotage. Fast-hardening glue, reactive or sticky acid (for accelerated rusting), flammable chemicals (napalm or thermite), and metal spikes are the primary weapons against barrels. All mentioned chemicals/materials can also be applied to other parts of a weapon system. The mission is to apply any method necessary to deactivate weapons permanently.

I have been thinking about Cyberwar 3.0 for a while and what it could mean if this concept is taken seriously and implemented worldwide. With weapons that target rifles, tanks, etc., Cyberwar 3.0 could enforce peace among humans in most parts of the world. Civil wars and the way they are fought could be stopped. The distribution of weapons of war among humans could be reverted, particularly among civilians. There are 75-100 million assault rifles of the type AK-47. This weapon is popular among non-state actors, like paramilitaries, insurgents, and terrorists, due to its low cost and ease of use. It has been used in many conflicts around the world. But if carried in the open, it could become a target for microdrones disabling it.

Even if not implemented in every part of the world, it could make the concept of having safety in countries without a military a feasible idea for more countries. Costa Rica, Iceland, Grenada, Nauru, and Panama are demilitarized; still, they have coast guards and strong police forces to maintain public order and safety. I don't have a problem with the idea that many more countries follow them. Can these countries use their drones in covert, preemptive missions to destroy offensive weapons like rockets, cruise missiles, or bombers that could reach their territory in neighboring countries? Is a world like that more stable or unstable?

Getting rid of military weapons could save millions of lives. Does it endanger more lives? If "we could, would we"; do we want to live in a world where military weapons cannot be carried openly? What is then the next generation of deadly weapons?

Cyberwar 3.0 Drones

Drones for Cyberwar 3.0 are expected to be produced (cheaply) in very large quantities, potentially 10s or even 100s of millions, to have a drone-to-armed-human ratio of 10:1 or even 20:1 within confrontations. The goal should be that the surrender of anyone (unauthorized) armed is the only option.

Battle situations, missions, and environments differ before, during, and after a conflict. Therefore, it is likely that there will be a basic drone model that can be configured or retooled with additional capabilities so that the drone squads (or swarms) stationed close to their targets can change their swarm configuration depending on the mission requirements and adversary's assumed behavior.

The ideal drone configuration will likely be determined in battle simulations; they are (potentially) done within video games with humans as passive observers studying and learning what's best. These simulations will determine the trade-offs extending the basic design of the drones, e.g., how much computational power they will have, how much energy (battery) or energy harvesting from the environment is included, or how good are video, audio, and positioning sensors, or the mechanism to release its weapon or how it is carrying a payload.

To make Cyberwar 3.0 more tangible now, I need to speculate (a bit). Many configurations and designs are conceivable, so plenty of ideas could be implemented. For your benefit, I allow myself to be imaginative and describe how I envision the different operational deployment elements.

Mass-produced microdrones are small, 3 to 5 cm in diameter. The environment recharges their batteries via energy-harvesting components or more quickly via power hubs at retooling stations. Their autonomy is limited by algorithms that can't be covertly modified; humans can stop their missions, which limits their autonomy. They will have reliable kill switches that only their operator/controller can activate. Microdrones can easily be retooled with weapons like glue, acid, paint, napalm, thermite, sleep gas, darts, bullets, etc. Depending on the received tool, a microdrone will be part of different (sub-)swarms. Microdrone squads are organized like military units consisting of drones with different specializations. Each special group of drones, defined by the same tools or weapons, is then part of a sub-swarm.

The Cyberwar 3.0 Drones could operate in 3 main modes: (a) they move, (b) they wait/hide/prepare, and (c) they sabotage.

Having microdrones moving between locations alone would be too inefficient. Instead, drones are stored, densely packed in small containers, and carried by drones over countries' borders to the deployed locations. These containers serve as holding hubs during the wait or stand-down periods. For their operations, these microdrones could quickly be released from these camouflaged (movable) containers.

Being too close to expected battlegrounds is potentially too risky, and being too far away makes them useless. For the last mile, to the places of battle or operation, it is advisable to have special transportation drones that could serve as small troop-chopper transporting microdrones to the staging area for their missions. Transportation of smaller units gives more flexibility in quickly deploying troops to multiple deployment zones; this will increase confusion and pressure from a highly coordinated and adapted attack. When carried, microdrones' valuable energy is not wasted but saved for their mission.

Additionally, drones carrying other drones could be turned into a scenario in which even smaller drones (e.g., 0.5 cm diameter/fly-sized drones) are released. These kamikaze mosquitos or nanodrones are less detectable and have a shorter reach. They could have needles to sting soldiers through their clothes and inject potent drugs that incapacitate them, e.g., with a knock-out dose, a few milligrams of anesthesia. These nanodrones would probably use different physical principles to move through the air than a rotor. Also, their energy/battery may only hold for less than a minute. Even if they are cheap, their technology is likely advanced enough to have them protected after their use, i.e., these nanodrones are self-destructive or "ambulance drones" pick them up automatically for being reused later. However, these nanodrones could also protect rooms by attacking surprised assailants carrying weapons.

A rough estimate is that between 500,000 and 1 million microdrones could be stored in a 40ft (large) shipping container. Based on that, the entire invasion army of drones with its supply/support could be delivered in less than 100 large containers. It seems also feasible that 36 hours after the drone's release from international waters, larger transportation drones could bring them to their final deployment destination while avoiding possible detection, i.e., by moving, e.g., at night and being additionally camouflaged. Pioneer drones prepare the routes. They organize and operate (power) refilling stations and, if necessary, create ambient noise days before so that typical drone noise cannot be detected. The route would go through very low-populated areas. Still, police stations or military posts could be put to sleep by odorless gas. All fixed anti-drone/detection equipment or their connection to a larger detection network could be sabotaged or temporarily disabled.

Autonomy requires computational resources and energy to operate it. Identifying targets is challenging, but I assume not more difficult than face recognition. Also, aiming reliably to a precise point where the drone can create (maximum) damage to a weapon is challenging. Comparably low-speed bullets or darts fired by the microdrone could be misdirected and wasted; therefore, drones would need proximity, i.e., microdrones must touch the target or get within a 1-meter combat zone or even a 10 cm fire zone with their targets. Doing unpredictable flight patterns around people or targets and then going into an optimal shoot position is not a problem. Having 5 or 10 microdrones doing this is a high-stress situation for soldiers, but it would make no difference to the drones.

Microdrones are expected to fire only a single bullet or dart. If the muzzle of a barrel is moving, it is unlikely that the drone's targeting systems have a clear-enough target. Human movements could be slowed down by a gas that could put them to sleep. The movements or the position of the muzzle or other weapon parts can be calculated and predicted by the drone. With proximity, high-precision optics is not required for aiming reliably. More important, attacks on soldiers or military equipment should always happen as a surprise attack: No warning, maximize confusion, put as many adversaries to sleep as possible, and then damage as much equipment in the shortest period, preferably redundantly in different ways.

When soldiers start using tennis-racket-type fly (or drone) swatter to counter drones harassing them, they may give their weapons less attention; this is then exploited by a more specialized drone squad going directly after the weapons. At the same time, drones with needles could attack from behind and sting and drug them with non-lethal doses of anesthetics. If these drones create some pain, soldiers will fear them even more and protect themselves, not their weapons.

Drones should be able to camouflage themselves based on the environment and conditions under which they are being used. Camouflage is done with paint

or with skin that could change its color. Also, drones' casing and rotors could be made of non-reflective, transparent materials like special (lightweight) glass or plastic. Rotors create noise that cannot be fully suppressed, but sound-generating drones could create enough other superimposed noise so that humans won't hear an army of drones coming before it is too late. Once in proximity, this additional sound can be turned into a weapon that increases confusion and fear.

Although supply could be provided via drones, there is an advantage of being less dependent on them. Therefore reused war material and repaired drones (e.g., new rotors, batteries, etc.) are helping an invasion force of drones to operate longer within enemy's terrain. Making drones reliable and their energy (stored in batteries) generated close to the deployment hubs could reduce the supply volume significantly.

The communication among a squad of drones, i.e., its internal command and control, could be based on 5G microcells. When communicating at that speed, the swarm could delegate computational tasks to special drones with more computational resources or memory. Having a swarm of drones seemingly operating as a single organism doesn't mean that all drones are clones. They could use other forms of self-organized, adaptive planning and decision-making with (some) centralized/specialized components. These components could have backups and distribute/decentralize some of their tasks. E.g., barrel/weapon detection, target selection, tactical battle planning, weapon usage, or attack orders could be done by non-engaging drones in the background. Dedicated observer drones could detect armed personnel and weapons. Early on, kamikaze drones could attack jammers that try to disrupt communication among the drones.

The decentralized deployment of millions of drones in 10s thousands of locations requires a high-speed data connection of the drone hubs via directed microwave or laser with the global command and control system. There might be a chance that some of these hubs are detected, but they are movable and can be relocated to prepared beta or gamma sides. Still, hubs should be sufficiently camouflaged; they must take active and autonomous actions to remain undetected and hidden within enemies' terrain.

Other Cyberwar 3.0 Attack Scenarios

Cyberwar 3.0 could be used offensively; It could (theoretically) destroy, e.g., the entire offensive weapon system and program of North Korea (DRNK). I write this because these are the consequences that security analysts will immediately see, and they will spell that out.

Using microdrones against heavy-armored adversaries is not different from using them against rifle barrels. Rocket launching systems and tracked vehicles can be sabotaged with well-placed thermite charges close to tires, tank chains,

gas tanks/lines, lines for breaking fluids, or electrical power lines. Rockets are very sensitive to sabotage. If something tempers with their nozzles or gas pipes, they are quickly useless and dangerous in their handling. Countermeasures against drones could be studied, and weapons countering countermeasures could likely be created by 3D printers near the drone hubs based on instructions from consulting experts. Defenders are surprised and have likely no chance against an army of flexible microdrones.

All weapons, including nuclear weapons, are useless as long as they are in bunkers. Also, enemies' ammunition depots and spare part storages are prone to sabotage with drones. Microdrones could be let in covertly by disgruntled personnel. Once (disgruntled) soldiers or officials are caught alone and turned into informants or collaborators. Like Cyberwar 2.0, low- and mid-level workers/people could give hints or access to hidden inventories, storage places, or laboratories. They need to open some doors: starting with the room for CCTV surveillance or internal power or communication switchboard. Internal equipment and infrastructure could be made useless by drones spreading napalm on screens or keyboards and burning them down. Napalm or thermite in ammunition depots could do the same. All these missions are kamikaze attacks by swarms of cheap drones.

It is known that the DRNK has a lot of equipment in bunkers and even mobile in underground facilities or tunnels; these capabilities are all static targets that can be studied and exploited. Drones could patiently wait until closed doors are opened or vehicles with weapons try to leave their confines. Or they could use their thermite to close the main doors permanently while waiting patiently at the secondary exits where the soldiers surrender.

Besides barrels and military infrastructure, specialized microdrones could attack people and drug them or blind them via sprayed paint on soldiers' goggles or glue on the openings of the gas mask, making it less useful for keeping it on. Once taken off, other drones could spray some odorless knock-out gas close to soldiers' faces or sting them with needles that would drug them in seconds.

It is a reasonable conclusion that Cyberwar 3.0 would deactivate all assets used by DRNK that threaten its neighbors, including all rockets, long-ranging artillery, and nuclear, biological, and chemical weapon capabilities. It is assumed that the superpowers have already sufficient intelligence on DRNK to get Cyberwar 3.0 assets focused on the relevant offensive military capabilities. Once stationed, these microdrones could autonomously sabotage all heavy military equipment, including airplanes, military vessels, and communication nodes/equipment used by the military. With enough time before starting the above actions, also submarines could be sabotaged.

Another scenario is using Cyberwar 3.0 in civil wars, e.g., Syria. Weapons, communication hubs, and ammunition depots can be destroyed, and the command and control of the current regime over their military, security, and administration could be significantly reduced. The unrest in these countries will likely

remain; only the methods of killing will change. Instead of military weapons, we would see more IEDs (improvised explosive devices), suicide bombings, or chemicals all used to continue that conflict. What is required is a solution that fills the power vacuum; without that, Cyberwar 3.0 is not a comprehensive technical peace solution.

Angry people and a destroyed country need a new beginning, a restart. The question is only: how? And what's next?

Aftermath of Cyberwar 3.0

Once a country like North Korea has lost its offensive capabilities, Cyberwar 3.0 drones would go after armed soldiers or anyone carrying a handgun openly or having a certain uniform. However, what happens next is certainly speculation. I will call it a possible scenario of how a regime change could play out. The aftermath will likely depend on the prepared decisions for the hours and days following the sudden disruption of the previously dominant political authority. The immediate aftermath of a victorious Cyberwar 3.0 is more important than any other event within that war.

Drones could deter military personnel from being outside their barracks, which means the defacto end of the old regime. Additionally, at the same time, police forces and the prison system are being attacked by drones. The old way of enforcing order is being disrupted. Prison guards are intimidated to set prisoners free, independently of what they did. Law and order will later be established based on fair legal principles despite its risks of liberating all prisoners.

Getting in touch with the population is the next challenge, but it will be among the most essential steps. Cyberwar 3.0 tools will not collect sufficient intelligence on each citizen, but drones and distributed flat/small message screens (solar powered, for being more reliable) can communicate with the country's inhabitants. One screen per family would mean about 10 million screens are distributed to its (DRNK) inhabitants within a few days (hopefully done in 1 day). This task could be done army of slightly larger microdrones (8 to 10 cm diameter). These drones can carry these screens and make basic contact with the citizens. This screen is essentially a (basic) smartphone but operated initially in an energy-saving emergency mode. Power-supply cable/adapter will be provided later.

The screen's message to the citizens is to be calm and to listen to essential instructions. These screens ask questions (likely textual Q&A) so that the new administration that will take charge within a few days could start from a foundation of sound information. All citizens are instructed to abstain from retaliation against their former suppressors. Vigilante justice will be detected by drones and later prosecuted and punished by jail.

People are addressed as individuals via the screen - dialogs are scripted and handled by its software automatically. Many are unsure or frightened, but their

lives must go on. Once the old regime or order is gone, filling the power vacuum is significant. Losing this chance initially could cause crime and anarchy; violence could destroy the tools and infrastructure needed to rebuild the country. As a beneficial source of information, this screen fills this vacuum with practical guidance. It will show and teach all people that bad behavior will have (later) consequences for them. Their world will change irreversibly for the better if they comply with the instruction.

It is expected that leaders in all communities will be identified from their answers. These identified leaders are then taught and instructed to follow certain basic rules. They are asked to take charge of their local community and spread optimism and hope about what will come next. These instructions and messages should prevent society from collapsing into anarchy or unorganized mobs who express their anger.

People involved with the old regime are instructed to lay low until law and order can be guaranteed on the street. Plans should be worked out on how public safety and the economy could restart quickly. From other failing countries, we know that small business owners within communities start relatively quickly managing the scarcity. A lack of trust, information, and communication prolongs scarcity. Reliable communication and useful information could take the edge off these problems.

Therefore, a next-generation mobile network should be ready to be rolled out as portable components (including antenna and backend components) within a week of the regime change.

The provided (basic) smartphones could be used to educate and cultivate people even further. These services should be free within the first few months of this transition.

Soon, the responsibility for infrastructure and previously governmentally-run businesses is transferred to groups of people that can manage them. The original sponsor for these components that helped in the transition would remain as a minority owner who could later receive a profit share.

External experts are primarily mentors for the new management team. These experts are being trained to deal with a restart and radical transformation of an economy. They should help to establish a more participatory culture. People motivated to take charge of their futures may alleviate regrets about living under their former conditions, even though many will be scarred for the rest of their lives. If this transition is doable remains to be seen - it is considered an alternative proposal to what failed in past and current nation-building efforts.

Today, the aftermath of a conflict is handled differently: don’t prevent the chaos; manage it with welfare help when it becomes unbearable to watch it. The new idea is to have a managed aftermath without a power or information vacuum.

We can use the advantages of smartphones and access to external artificial intelligence (AI) that could help people deal with their problems more personalized than what the Internet of publications currently accomplishes. This development assistance could unleash economic forces much faster. We could create better results with AI; it's better than what we could have done in the past. I doubt this new concept is more expensive than the old way of handling chaos.

In preparation for (natural) disasters, Cyberwar 3.0 drones could also be used. It is worth having an emergency stack of smartphones and equipment to establish phone services quickly. A large supply of cheap devices could be available for almost instant shipping. The damage that nefariously distorted information can create in the aftermath of disruptive events is underestimated. Propaganda and PsyOps works. It might be too late if a foundation of trust is not set right from the beginning. Controlling the narrative with truthful (beneficial/independent) information is essential for building trust.

Regarding the destiny of the old regime, they will quickly realize that they have no tools to keep on with their repression. Also, striking out militarily against neighbors is too late. The old leaders and their top henchmen may flee, or preferably, their travel movements are detected, and special force missions are designed to prevent them from leaving their country. Unfortunately, direct intervention with special forces is unlikely. But still, it is conceivable that drones are used, i.e., instructed by the ICC (International Criminal Court) to organize the orderly arrest of the previous leadership. With drones watching all leadership buildings and no vehicle or plane left to use, they may not have any other way out than surrendering.

Defense against Cyberwar 3.0

It was already mentioned that we have a significant commercial drone problem and that people can use these drones as weapons against others. We trace their ownership back to the culprit and tell ourselves there is no qualitative difference or advantage in using drones over other weapons. Owners are responsible for their property. People can even be made accountable as an accessory to a crime if their property was part of a crime and not sufficiently under lock.

We will adapt to drone warfare in the same way as we adapted to car bombs. Deploying substantial defensive measures against military and civilian targets, even extensive netting or fencing, could become justified, similar to how concrete barriers around secure buildings is now common practice to protect against car bombings. Security measures have evolved. My concern is that they work and are worth it.

So far, countermeasures against drones include missiles, guns, electronic jammers, cyberweapons, high-powered microwaves/lasers, and passive defenses such as nets.

Under the assumption that we already have a Cyberwar 3.0 drone program that provides cheap basic drones, I believe using drones against drones is the most cost-effective way of dealing with this threat for regular targets like office buildings. I imagine that drones could become pretty good in drone dog fights. I believe a combination of microwaves, lasers, and defensive drones should be used for high-value military or political targets.

Drones as countermeasures could be stored in containers; they release microdrones quickly and be installed/deployed effortlessly. These defender drones would directly fly to attacking drones and use, e.g., spray, yarn, or net to trap the other drone, even larger ones. The method of attacking and defeating drones should be easily changeable as an arm-race between attackers, and defenders must be expected.

Detection of drones and keeping them apart from birds is as important as disabling or destroying drones. Therefore optical and acoustic sensors should be used to protect areas where autonomous drone attacks are expected for various reasons.

What's the Catch?

Living in a world where weapons are attacked as soon as they are shown in the open is a very radical concept. Is this utopia or dystopia?

I believe it is possible to create Cyberwar 3.0 drones and station them worldwide for well-intended offensive purposes; domestically, they can be used for defensive causes. I believe Cyberwar 3.0 can discipline or punish overly aggressive neighboring countries and end civil wars. But it won't end terrorism in these countries. It could give countries only a renewed chance to solve their conflict. Cyberwar 3.0 alone won't solve conflicts.

Once a country deploys defensive Cyberwar 3.0 drones, it does not need to be concerned about an invasion anymore. If aggressors would still try it, they would predictably lose their weapons. Assailants may try to occupy some territory, but what method can they use to force inhabitants into compliance?

With face recognition, Cyberwar 3.0 drones could accept the good guys carrying guns. Even civilians could be accepted as good guys. These drones could also accept exclusion zones like training ranges or hunting areas in which rifles or handguns are allowed.

Drones could easily turn humans' lives into living hell. Humans eventually stop harassing others. Drones, don't. Their energy runs low, but after recharging, they start again. No end in sight unless it's destroyed, or you lock yourself in for a very long time, get rescued by others, or find a way that the drone accepts their surrender. Drones are still controlled by humans, even if they are called autonomous.

If I would speculate on what kinds of agile, small-sized technology will be available within the next 5, 10, or 15 years, then I immediately lose faith in the

engineering or resilience of heavy-armed equipment. What a waste. I don't believe they could withstand microdrone sabotage. Drone attacks are surprise attacks (in time, location, conditions, and method). If I see pictures of fighter jets or tanks or rocket launch systems, I believe I could find 50 to 100 weak spots that could be worth exploring if sabotage by glue, acid, paint, or drops of napalm/thermite (fire) could turn these dinosaurs into junk. I can extrapolate some technological capabilities into the future. Often, (civilian) capabilities are available much sooner and much better than expected. We have then 10s or 100s of billions or even trillions of dollars in military hardware that is suddenly worth nothing. Due to the acceleration of technology, expensive stuff is likely junk when ready for delivery.

Within 3 to 10 years, I could see commercial technology with some essential Cyberwar 3.0 drone features as open-source projects; this could seriously challenge nations in their weaponization posture.

In 2-5 years, I could imagine that government-funded defense programs deliver Cyberwar 3.0 systems that are battlefield ready; whether this is enough to be deployed against Russia, DRNK, or Syria is unknown. However, pacifists should be motivated to work on (non-lethal) AI/drone weapons that destroy weapons.

I believe Cyberwar 3.0 drones will be developed because several countries will demand defense products that help them to defend themselves against occupation by a much stronger neighbor. China has several concerned neighbors; Japan could be motivated to become even a market leader in Cyberwar 3.0 based on their still prevalent pacifistic attitude. The same could apply to Europe. Being competitors in these peaceful technologies could give the world some hope that we don't waste resources on military junk but on versatile drone technology that can also be used in many other useful applications, e.g., planting trees, etc.

Cyberwar 3.0 could prevent invasions; military forces could be rejected without large amounts of casualties on both sides. Cyberwar 3.0 drones could blend in within country's infrastructure and open terrain without exposing signs on where the 1,000s or 10,000s of drone nests are located. Missile defense systems like the Iron Dome or Patriot systems are defensive systems and should be deployed alongside defensive Cyberwar 3.0 drones.

Countries accepting Cyberwar 3.0 as a defensive technology could become members of a like-minded defense alliance like NATO, which then could commonly control the use of these weapons.

There is a catch.

The catch is that all these Cyberwar 3.0 weapons must be protected and hardened against cyberattacks and tools expected from Hacker-AI and within Cyberwar 2.0. If drones are vulnerable to hacker attacks, we could have a swarm of autonomous lethal drones controlled by cyberterrorists (or other adver-

saries). Vulnerable drones are weapons of mass destruction (WMD). Unfortunately, I must also extend this statement to our commercial (hobby) drones. However, the same concern applies to other remotely controllable weapons. The required protection is doable, as the next chapter will show.