

# The Ten Rules of Masking

By Colonel John Antal, US Army (Retired)



**M**asking is the full-spectrum, multi-domain effort to deceive enemy sensors and disrupt enemy targeting. A metaphor for masking is an archer firing on a target. The archer must first sense the target, then loose an arrow with precision to hit the target. If you blind or distract the archer, you are deceiving the sensor. If you cause the archer to miss, even though the archer sees the target, you are disrupting his aim. If somehow you can deflect the arrow, the archer must try again. Masking is about deceiving the archer's ability to identify and locate the target and then disrupting the archers aim or deflecting the arrow so that he misses the target.

Masking is one of the most challenging skills of multidomain operations (MDO) and the ultimate test of training and leadership. For masking to work, every echelon of command must understand and practice it. Vanishing from enemy sensors and disrupting the enemy's kill chain demands unwavering focus, new battle drills, innovative Tactics Techniques and Procedures (TTP), and the right tools.

Today, war is an intense contest between hiding and finding. To be detected by the adversary's sensors is to be targeted and killed. In the modern battlespace, there are no sanctuaries. After decades of uncontested air dominance and wars of counter-insurgency, the US military is unskilled at hiding in plain sight and conducting dispersed operations that deceive and confuse the enemy. With the proliferation of satellite systems, balloons in the stratosphere, and high-definition multispectral sensors on a host of drones in the air, no place should be considered "safe" and out of the observation of enemy sensors. With the accelerated development of long range precision fires and drones, no location in the battlespace should be considered out of the range of the enemy's fires. Our enemies, even some that we might consider second-rate militaries, possess extensive arrays of advanced sensors capable of

monitoring targets in real-time throughout the battlespace. The unblinking eye of these sensors surveil nearly everything. These real-time sensors link to shooters, such as artillery, drones, missiles, and aircraft. The enemy's sensor network is designed to find, target, and enable long range precision fires, drones and aircraft to kill you. You must take extraordinary efforts to mask from these enemy sensors and precision fires.

There are five sensing areas that every warfighter must consider: optical, thermal, electronic, acoustic, and quantum. The first four are the focus of your masking efforts in today's battlespace. The fifth, quantum sensing, is still emerging, and will require its own set of rules.

Borrowing advice from Sun Tzu, the ancient sage of war, masking has ten principles in application. Five deal with deceiving enemy sensors and five with disrupting the enemy's targeting system. Follow these ten principles to mask effectively in the modern battlespace. The path to becoming a ghost on the battlefield is guided by these ten principles. Embrace them, internalize them, and then adapt, improvise, and unlock the secrets of masking.

**1. Know the Enemy Sensors:** Sun Tzu said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Deceiving the enemy's sensors starts with knowing what sensors the enemy has and directing your masking efforts against his high-payoff sensors. Understanding how the enemy is seeing the battlespace provides the keys to deceiving his sensors.<sup>1</sup> Ask questions like these: What are the enemy's primary day and night sensor systems in the optical arena? What enemy systems are armed with thermal sensors? What systems does the enemy have to conduct detection in the electromagnetic arena? What systems does the enemy have that use acoustic sensors? Find answers to these questions and take action.

**2. Master the Art of Optical Camouflage, Cover and Concealment:** Sun Tzu said, "All warfare is based on deception. Hence, when able to attack, feign inability; when strong, act weak; when near, make it appear far; when far, make it appear near." A means to accomplish this is by camouflaging. Camouflage is a discipline that you must embrace. **Camouflage is life. If you do not camouflage effectively, you are asking to be seen and hit.**<sup>2</sup> By mimicking textures, colors, and patterns, camouflage aims to trick the eye and sensor, transforming an object into an

---

<sup>1</sup> What sensors does the enemy use at the ground level, in the atmosphere (drones, balloons, aerostats, aircraft, and missiles); in near space (the stratosphere and mesosphere where balloons and aerostats operate); and in outer space (usually designated by the Kármán line, an altitude of 100 km (62 mi) above sea level, where satellites operate)? A complete masking plan would include specific actions to deceive enemy sensors in each level.

<sup>2</sup> How battlefield camouflage works: <https://www.youtube.com/watch?v=kigJ2jx15Go> and The Art of Deception: Advanced Military Camouflage: <https://youtu.be/OTWCbaUMkeI>

extension of its environment. Use shadow and shade. Do not skyline. Break up surface images with rough patterns of netting or natural camouflage. When possible, reduce sudden movement as this will catch the eye of the sensor. Camouflage aims not just to conceal an object, but to seamlessly integrate it into its surroundings, making it virtually indistinguishable from its environment. More than hiding something from sight, camouflage seeks to disguise it as part of the background, fostering visual harmony and deception. Evading detection by enemy optical sensors, be it from drones, satellites, or ground observation, requires a multi-layered camouflage approach. First, use every means to blend into the existing terrain. Use forest, jungle, restricted terrain, and urban terrain to hide from enemy sensors. **Never** set up a Command Post (CP), supply depot, maintenance operation, or fighting position in an open, unconcealed area. Second, master the art of strict camouflage discipline and require each warfighter and system to be camouflaged appropriate to the surroundings at all times. When required to remain in one position for hours or days, dig in critical systems and critical infrastructure such as CPs and supply depots to avoid detection from overhead sensors and provide protection from enemy fires. Third, proactively gather intelligence on enemy sensor capabilities and deployment patterns to avoid areas with high sensor density or adjust movement tactics accordingly. Fourth, constantly view your own position from the ground level **and from above** with drones equipped with cameras to see how the enemy sees you. With this knowledge, modify your masking efforts accordingly. Fifth, ask these questions: Have I camouflaged effectively to hide from enemy optical sensors? Am I using the terrain in the best way possible to seamlessly merge with the surroundings? Does my optical signature look like a conspicuous target that sticks out in the battlespace? Find answers to these questions and take action.

- 3. Master the art of Thermal Camouflage:** Sun Tzu said, "Move like a fox and be as secret as the night." Take measures to hide in the IR (Infrared) spectrum.<sup>3</sup> Day or night, modern armies are equipped with thermal sensors to see beyond the optical spectrum. The primary means to defeat enemy thermal sensors is to blend into the thermal background by reducing vehicle and equipment thermal emissions using insulation and shielding.<sup>4</sup> To become expert at this you must consistently observe your positions and equipment with thermal sensors similar to what the enemy is using. These observations should be from the ground level and by drone, from above, as top-attack is a preferred method of modern combat. Natural terrain such as forests, jungle, restricted terrain and urban terrain, offer natural insulation and shielding from enemy thermal sensors. Heat management, such as turning off non-essential equipment, can help reduce the heat signature. Using tarps and covers that do not touch the heat source but provide a layer of thermal obscuration can help shield the thermal signature for periods of time. Identify the environment, weather, and sensor crossover points that occur each day, usually at dusk and dawn, when

---

<sup>3</sup> See: IRR Camouflage explained - Basic infrared knowledge: <https://www.youtube.com/watch?v=lfUhVy-4CSY> and "How To Hide From Military Drones" <https://youtu.be/Zcj5ZeEn6qU>

<sup>4</sup> "How to Hide From Drones: Lessons Learned in Modern War" See: <https://www.youtube.com/watch?v=gYVpvXNiYi8&t=26s>

the ambient temperature of the environment starts to approach the average temperature of the object trying to remain hidden. In order to move like a fox and be as secret as the night in the thermal spectrum, master the art of thermal camouflage by learning how to use thermal crossover periods, barriers, and thermal management. Ask questions like these: What does my thermal image look like right now? Is my thermal image as seen from above clearly visible to enemy sensors? Is my thermal signature effectively blending with the surrounding environment? Can I turn off, conceal, and cover equipment that emits a higher temperature than its surroundings? Find answers to these questions and take action.

- 4. Master the Art of Electronic Deception:** Sun Tzu said, "Appear weak when you are strong, and strong when you are weak." Electronic warfare is central to modern war. The war in Ukraine emphasizes the vulnerability of command posts (CPs) to electronic detection and targeting. The Russians have a robust reconnaissance-strike complex that is skilled at identifying targets in the electromagnetic spectrum and then attacking them with massed fires. In a similar way, our forces can be located by Russian, Chinese, Iranian and North Korean EW systems.<sup>5</sup> To be detected is to be killed. Our electronic networks must be hard to find and harder to hit. First, we must "see" our own networks in order to reduce and obfuscate their signatures.<sup>6</sup> Very high frequency (VHF), ultra-high frequency (UHF) and satellite communications (SatCom) tactical radios are easy to detect. Employing high frequency (HF) radio software-defined systems (SDR), along with disciplined transmission techniques and operating procedures, can decrease the probability of detection.<sup>7</sup> However, with the right EW equipment it is possible to identify nearly any transmissions made across the electromagnetic spectrum. Minimizing transmissions, therefore, is the surest way to reduce the signature. To counter electromagnetic sensors, we must develop and employ strong electronic signature discipline. Some solutions can also be found in going analog. During the fighting in Ukraine in 2023, many Ukrainian units used "Cold War" era wire-enabled field phones to connect

---

<sup>5</sup> "The R-330Zh Zhitel jammer, which can reportedly shut down all GPS, satellite communications and cellphone networks in the very high frequency and ultra-high frequency bands within a 25-kilometer radius." Tamara Moskaliuk and Brandon Malatest, "Russia Versus Ukraine and the Role of Software-Defined Radios," The CyberEdge by Signal, Feb. 1, 2023. See: <https://www.afcea.org/signal-media/cyber-edge/russia-versus-ukraine-and-role-software-defined-radios>

<sup>6</sup> "One such capability [to see your electronic signature] is the Spectrum Situational Awareness System (S2AS) that is being developed by Program Executive Office Intelligence, Electronic Warfare and Sensors. It is a planned new start in fiscal 2025 envisioned to be a commercial-off-the-shelf solution that will provide sensing and visualization of what units look like in the spectrum." See: Mark Pomerleau, "Army Wants to 'Reimagine' Electromagnetic Signature Management," DefenseScoop, Oct. 11., 2023. <https://defensescoop.com/2023/10/11/army-wants-to-reimagine-electromagnetic-signature-management/>

<sup>7</sup> "HF Low Probability of Intercept (LPI) is a tactic that rapidly varies the power output and frequency of HF channels used to transmit, greatly reducing the likelihood of detection.<sup>9</sup> With appropriately trained personnel, certain maritime communications systems are currently capable of employing HF LPI." Brian Kerg, "Winning the Spectrum," Center for International Maritime Security, Aug. 7, 2020. See: <https://cimsec.org/winning-the-spectrum-securing-command-and-control-for-marine-stand-in-forces/>

communications within static positions. Enemy EW systems can detect radios and mobile phones, but not old-style field telephones.<sup>8</sup> Another means is to employ “radio listening silence” to decrease radio emissions and not to allow the use of personal mobile phones in the battlespace. Never allow friendly personnel to carry and operate civilian mobile phones as these are easy to detect and target. Be able to “Go Dark” (turn off all electronics) for specified periods of time, especially when units are occupying Assembly Areas (AAs). Use Electromagnetic Countermeasures (ECM) to trick or deceive enemy sensors; Electronic Signature Management (ESM) and Cyber Security.<sup>9</sup> Employ cybersecurity measures to protect communications networks; and spread false information on enemy and civilian networks to confuse the allocation and direction of their sensor placement. This includes counter radar techniques (deflect or absorb radar waves), jamming and spoofing, and cyber security and deception. Understand your weapons and their electronic signature. For example, the US Army’s new Active Protection Systems (APS) mounted on the M1A2SepV3 Tank to shield against incoming missiles has a hidden downside: they light up like beacons in the battlespace to enemy EW sensors. Radar has to reveal itself to work. Using mini-radars, the APS boosts survivability from direct threats but also increases a unit’s electromagnetic footprint, potentially attracting top-attack munitions. Will US tank units turn on their APS when contact is imminent, or leave it on all the time? Think about and practice emissions control (EMCON), consider unplugging and using communication windows for reporting at predesignated times, and maximize mission command. Ask questions like these: Are my radio and digital systems easy to discover by enemy EW systems? Do my units have strong electronic signature discipline making them harder to locate? Can I communicate by other means that are more difficult for the enemy to detect? Find answers to these questions and take action.

- 5. Master the Art of Acoustic Deception:** Sun Tzu hinted that you can deceive your enemy with sounds by making noise in the east while striking in the west. Drone mounted acoustic sensors pose a growing threat to military ground units in the modern battlespace. Enemy drones are now equipped with sound sensors that can register and locate noises such as cannon fire and the sound of generators. These acoustic sensors are cheap, passive, and effective. Reducing the acoustic signature of equipment, vehicles and weapons is difficult, but not impossible. First, know the level of noise that you are emitting by paying attention to your acoustic signature and take action to reduce the noise level or mask it with noises in other areas. Turn off unnecessary equipment. If you must be stationary, dig in generators to muffle their sound. The best case is to be mobile, under armor, and not become a stationary target. Be prepared to shoot and scoot, especially for artillery and tank systems, so that if you fire a weapon several times you do not linger in the area for long after firing. Integrate electronic warfare systems that can jam or disrupt enemy acoustic

---

<sup>8</sup> Jonathan Beale, “Ukraine war: How old tech is helping Ukraine avoid detection,” BBC News. May 3, 2023. See: <https://www.bbc.com/news/world-europe-65458263>. Also see: TA-1/PT [https://www.radionerds.com/images/2/22/TM\\_11-5805-243-13.PDF](https://www.radionerds.com/images/2/22/TM_11-5805-243-13.PDF)

<sup>9</sup> See “The Invisible Battlefield: Electronic Warfare, Explained” - [https://youtu.be/2L\\_2ITqvRQA](https://youtu.be/2L_2ITqvRQA)

sensors, temporarily creating blind spots or hindering their ability to track specific sounds. Use sonic decoys that you can leave in place to operate autonomously to draw enemy sensors to false positions. Ask questions like these: Can I reduce my noise signature by turning off or dampening the sound of my equipment? Do my units shoot and scoot, minimizing loitering time, or are they staying in one location too long after shooting? Find answers to these questions and take action.

**6. Master the Art of Disrupting the Enemy's Targeting System:** Sun Tzu said, "Be where your enemy is not." Sensors locate targets for precision, smart or area weapons. Once sensors identify their prey, precision weapons can be dispatched to hit the target. If you can disrupt the enemy's targeting system, throwing off his aim, you can survive to continue your mission. To disrupt the enemy's targeting, you must know the steps of his kill chain for his primary weapon systems such as artillery, rockets, drones, and other indirect fire systems. Most sUAS in use today have a range of about 20 km/12 miles, but that range is increasing with technological improvements. In the war in Ukraine, First Person View (FPV) drones are especially effective against supply trucks and armored vehicles. To counter FPV drones, Ukrainian vehicle and howitzer crews have erected improvised nets, chain-link fencing, and mesh screens to stop Russian Lancet loitering munitions and FPV drones. Many factors influence the success of these screens and they have no effect against heavier and faster missiles or artillery shells. "The most effective countermeasure to tactical kamikaze drones is ECM. In the case of Lancet, jamming is required of both the GPS and TV-command signal. FPV drones only require jamming of the TV signal."<sup>10</sup> Multi-spectral smoke can also interfere with incoming precision-guided missiles or drones. Using disruptive TTP, such as an "Incoming Drone" battle-drill, where vehicles execute unpredictable movements like weaving, zig-zagging, or even reversing, may cause the drone or missile to miss its mark, whereas doing nothing is a recipe for disaster. Ask questions like these: What are the steps in the enemy's kill chain and how can I disrupt it? What can I do at the final stages of the enemy's kill chain to make him miss his target? Find answers to these questions and take action.

**7. Always Use Decoys:** Sun Tzu said, "Set up decoys and feign confusion, and give the enemy the impression we are about to quit our position. Then select our elite mounted troops, and send them on ahead into enemy territory under a cloak of silence." Using decoys is a tactic as old as war, but many in the US military have forgotten how to do this. Decoys, both prefabricated and improvised, should be routine tools and can be employed in both offensive and defensive operations. Even the simplest decoys can cause the archer to see a false target and miss the real target. In the fighting in Ukraine in 2023, Ukrainian soldiers shoved sticks in the ground, put clothes on the stick and a helmet to create a simple an effective decoy

---

<sup>10</sup> Sergio Miller, "Countering Tactical Kamikaze Drones – Ideas Urgently Needed," Wavell Room, Oct. 13, 2023. See: <https://wavellroom.com/2023/10/13/countering-tactical-kamikaze-drones-ideas-urgently-needed/>

that drew Russian fire.<sup>11</sup> Not using decoys, however, is sheer laziness and a recipe for failure. Decoys can be physical (fake vehicles or CPs or saturating an area with radar reflective surfaces to overload enemy radar systems and create confusion); physical effects (such as smoke, acoustic decoys to mimic vehicle or weapon sounds, or thermal emissions from smudge pots or electronic thermal blankets that give off heat to attract thermal sensors); or virtual (electronic, such as fake radio messages or cyber spoofing, filling the enemy's common operational picture with hundreds of false positive sightings). A tiny, disposable decoy mimicking army radios or electronic signatures — something like the disposable Electromagnetic Warfare Decoy Emitter that can mimic the Electromagnetic Signature (EMS) of a tactical radio and double as a frequency jammer — could confuse enemy sensors, boosting battlefield survival for ground troops.<sup>12</sup> Decoy CPs and decoy CP emissions can be particularly effective in confusing enemy fires and targeting. Decoys do not need to be perfect but simply complicate the enemy's decision making and make him turn his sensors in the wrong direction. Routine use of decoys, whether prefabricated or improvised, offers tactical advantages by misleading enemy sensors and disrupting their targeting capabilities. Ask questions like these: What decoys can I deploy at each echelon of command to mask my positions? What decoys can I set up in the defense? How can I deceive the enemy with decoys in the offense? How many decoys does each unit create and deploy every day? Find answers to these questions and take action.

- 8. Confuse the Archer:** Sun Tzu said, "Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt." Confuse the archer to see threats that do not exist. In the modern battlespace, sensor deception and information warfare should employ creative tactics to exploit vulnerabilities in the opponent's sensor systems. The lack of any information, or too much false information, can confuse the enemy. At the Battle of Midway during WWII, the American Navy operated on radio silence, going dark on radio transmissions, before contact with the Japanese Navy. This blinded the Japanese to the close presence of the American Aircraft Carriers which then sprung a trap against the Japanese fleet.<sup>13</sup> Modern electronic warfare (EW) and cyberwar systems can provide similar confusion to the enemy today. We should practice this routinely. Dispersion is also a vital means to confuse the enemy. The target that sticks out, gets hammered. Two or four vehicles grouped close together in the battlespace may look like a platoon to enemy sensors. There will be many platoons in the battlespace and the enemy may look further

---

<sup>11</sup> Lilian Manasala, "Decoys and deception have long played a crucial role in Warfare," Business Insider, Nov. 24, 2023. See: <https://www.businessinsider.com/decoys-inflatable-dummy-tanks-ukraine-russia-war-military-strategy-deception-2023-11?op=1>

<sup>12</sup> Todd South, "A soldier-built Decoy Device Won this Army's Tech Competition," Army Times, Nov. 9, 2023. See: <https://www.armytimes.com/news/your-army/2023/11/09/a-soldier-built-decoy-device-won-this-armys-tech-competition/>

<sup>13</sup> Mark Munson, "The Battle of Midway, the Complete Intelligence Story," War on the Rocks, Jun. 3, 2016. See: <https://warontherocks.com/2016/06/the-battle-of-midway-the-complete-intelligence-story/>

before committing resources to destroy a platoon. Ten vehicles grouped together, however, are a target waiting to be hammered. Twenty vehicles grouped together around tents will bring down a rain of fire. Confuse the archer by dispersing your soldiers, weapons, and CP elements. Do not look like a target asking to get hammered. Ask questions like these: How can I disrupt the enemy's sensors through the unconventional positioning of my forces? How can I move forces in unexpected directions to mislead the enemy? How can I change my TTP to confuse the enemy? How can I build on the enemy's preconceptions to make him move or strike in the wrong place and time? Find answers to these questions and take action.

- 9. Blind the Archer:** Sun Tzu said, "In all fighting, the direct method may be used for joining battle, but indirect methods will be needed in order to secure victory." If the enemy sensors cannot see, the enemy's targeting system will fail. Study the enemy sensor systems, know how the enemy's ISR data is collected and networked, and find weaknesses in the enemy's information chain to blind his sensors. For example, radio deception and chaff were utilized during the D-Day invasion of World War II to trick German radar into thinking that the Allies were going to strike the Pas de Calais instead of the Normandy beaches. Modern means to blind the archer, using multi-spectral smoke, EW, and cyberwar efforts can produce similar results as physical chaff did during the D-Day operation. Scattering disposable IR lights, might spoof his top-down sensors, making the enemy perceive "targets" wherever these lights are positioned. Ask questions like these: What are the enemy's primary sensor systems? How can I blind these sensors? How can I manipulate the enemy sensor network to focus in the wrong direction, place, or time? Find answers to these questions and take action.
- 10. Kill the Archer:** Sun Tzu said, "Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." The slowest tactic is to stop the arrow. The victorious strategy is to kill the archer. The choice between stopping the arrows or killing the archer — to shoot down or jam the drone versus kill the drone operator — is a clear one. If you don't kill the archer the arrows will continue to rain down. During the Second Nagorno-Karabakh War (2020), Azerbaijan repurposed AN-2 Colt biplanes as unmanned, Remotely Piloted Vehicles (RPVs). They then filled each aircraft with explosives and flew them against the Armenian air defenses in the opening hours of the war. These RPVS were bait. Flying a medium altitude so that Armenian radars would be sure to pick them up, the Armenian air defense network turned on, identified, and then destroyed the incoming AN-2 COLTs. As the Armenians were congratulating themselves over this victory, their air defenses were identified by Azerbaijani sensors. Swarms of Azerbaijani Unmanned Combat Aerial Vehicles (UCAVS), loitering munitions, and precision missiles then attacked the Armenian air defenses. The repurposed biplanes had done the trick and blinded the Armenians to the true purpose of the attack, which was for them to turn on their air defenses in order to knock down the Azerbaijani attack. Rapidly, the Azerbaijani precision attack disintegrated the Armenian air defense network, killing the archer, and Azerbaijan secured air dominance over the battlespace. With air dominance,



Azerbaijan had set the conditions to win the war.<sup>14</sup> Ask these questions: How can we observe the enemy attack systems? How can we find, target, and destroy the enemy drone, artillery, and missile launch sites? How can we find, target, and destroy enemy drone, artillery, and missile ammunition depots? Find answers to these questions and take action.

These ten rules are designed to encourage you to think and discuss the concept of masking in the modern battlespace. Remember, there are no safe places, no sanctuaries. Assume that the enemy will see and target you. We must become difficult to find and much harder to kill. To put it in archer-like terms, your objective is to become impossible to be observed, to do anything you can to interfere with the archer's aim, to block the archer's arrows, and ultimately to prevent the archer from firing at all by taking him out. Skill, training, new gear, new tactics – it's all about masking your every move in this deadly new landscape. Masking is a mindset. Although better equipment is always appreciated, developing a masking mindset is more critical to deceiving the enemy's sensors and disrupting the enemy's targeting system than equipment alone. Most importantly, determined leadership is required to generate the discipline necessary to operate in this dangerous environment. Ultimately, the responsibility lies with leadership to train warfighters "to habit" in order to survive, fight, and win. Otherwise, there will be dire consequences. Lead. Reevaluate your training and preparation. In order to survive and win, adopt these ten rules and become the driving force that leads to success, ensuring that your leadership contributes to victory.

For more information on Masking and the changing methods of war, please see:

1. Georgetown Security Studies Precision-Guided Podcast – Book Talk: "Next War" with Colonel (ret.) John Antal - <https://georgetownsecuritystudiesreview.org/2023/11/20/precision-guided-podcast-book-talk-next-war-with-colonel-ret-john-antal/>
2. Squaring the Circle Podcast: <https://shows.acast.com/squaring-the-circle/episodes/discussion-on-the-future-of-war-with-colonel-r-john-antal>
3. *Next War: Reimagining How We Fight*: <https://www.amazon.com/Next-War-Reimagining-How-Fight/dp/1636243355>

---

<sup>14</sup> John Antal, *7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting*, Casemate, Feb. 3, 2022. p. 26. See: <https://www.amazon.com/Seconds-Die-Military-Nagorno-Karabakh-Warfighting/dp/1636241239>