SIMPLE SABOTAGE

- 2025 EDITION -

“One has a moral responsibility to disobey unjust laws.”

—Martin Luther King Jr.,

Letter from Birmingham Jail (1963)

THE SCOPE OF SIMPLE SABOTAGE

The purpose of this document is to define simple sabotage, outline its potential effects, and offer suggestions for inciting and executing it in today's world.

Sabotage can range from complex, technically sophisticated acts—requiring significant expertise and specialized tools—to countless simpler actions that ordinary people can perform in their daily lives. This guide focuses on the latter form. Simple sabotage typically doesn't demand specialized equipment and can be carried out by someone acting alone, possibly without ties to any larger group. These actions are often designed to blend into normal routines, minimizing personal risk and detection.

Where physical damage is involved, saboteurs may rely on items commonly found in offices, homes, or personal toolkits—everything from cleaning chemicals, adhesives, or small electronics, to a standard "maintenance" kit on-site. Targets of sabotage are typically assets that one can access naturally or inconspicuously: shared office printers, file cabinets, supply closets, or even server rooms if one's role permits.

Another category of simple sabotage relies on indirect methods, often harnessing mundane opportunities to make flawed decisions, behave uncooperatively, or subtly encourage others to do the same. An unwise decision might be as trivial as placing a frequently used office tool (like a USB hub or projector remote) out of reach, causing minor but repeated disruptions. A non-cooperative stance might entail consistently sowing confusion in team meetings, fostering arguments, or showing obstinate and unhelpful behavior. Even in normal circumstances, these human factors contribute to delays, inefficiencies, and confusion. By deliberately amplifying them, a saboteur can significantly disrupt operations while remaining difficult to implicate.

EXPANDING THE REACH AND IMPACT OF SIMPLE SABOTAGE

Acts of simple sabotage can arise anywhere—across offices, factories, digital platforms, or physical infrastructure. To maximize their effect, these activities should be refined to boost their overall impact, reduce the risk of being caught, and encourage more frequent instances. When practiced en masse, simple sabotage can become a formidable method of undermining an adversary's resources and logistics.

Examples range from slashing tires on delivery trucks or siphoning fuel from company fleets to more subtle actions like quietly corrupting database entries or repeatedly causing small but disruptive IT "glitches." Although each act alone may seem minor, collectively they result in wasted materials, manpower, and time. On a large scale, this continuous strain can meaningfully hamper the operations or morale of a targeted organization.

Such sabotage can also produce secondary advantages. Broad, low-level disruption will frustrate managers and security personnel, while each successful act can embolden the saboteur—and perhaps inspire them to collaborate with others for more ambitious activities. Additionally, the mere existence of widespread, small-scale sabotage can motivate people in compromised or occupied regions to identify and support a broader resistance effort, ultimately creating a more unified front in times of crisis or conflict.

MOTIVATING AND SUSTAINING THE CITIZEN-SABOTEUR

Encouraging citizens to adopt simple sabotage—and maintain these efforts over time—presents a distinct challenge. Acts of sabotage typically do not offer immediate personal gain; in fact, they often conflict with one's natural inclination to avoid waste or to appear competent. It takes consistent motivation, reassurance, and practical guidance for people to integrate such acts into daily behavior.

PERSONAL MOTIVES

Indirect Benefits: Individuals may not see a direct payoff for committing sabotage. Instead, they can be motivated by anticipated indirect gains—for instance, undermining an oppressive regime or hastening an end to unpopular workplace policies. These promises should be stated in concrete, relatable terms: disrupt server uptime to reduce invasive oversight, hamper shipments that reinforce exploitative conditions, etc.

Feeling Part of a Network: Because small, isolated acts may seem ineffectual, individuals need a sense that others elsewhere are doing the same. Broadcasting success stories or providing cryptic updates about "similar actions in neighboring offices or locations" can reinforce this solidarity. Publicizing the scale of sabotage—within reason—encourages more participation.

Sense of Responsibility and Leadership: Beyond indirect rewards or group identity, the strongest motivation arises when a saboteur feels personally accountable for teaching or inspiring others. By coaching colleagues or sharing instructions (discreetly, of course), an individual becomes more invested in ongoing sabotage efforts.

ENCOURAGING DESTRUCTIVENESS

Psychological Shift: Potential saboteurs often must reverse ingrained habits: instead of diligently maintaining equipment, they allow it to degrade. Instead of carefully lubricating gears, they let dirt accumulate. By viewing everything as sabotage-ready, they can discover countless minor acts that steadily degrade systems.

Range of Skill Levels:

A. Less-trained individuals need specific, step-by-step guidance (e.g., where to insert foreign objects in a copier or how to misconfigure a router).

B. Skilled technicians or "power users," such as IT staff or engineers, can devise their own methods once they've adopted a sabotage mindset.

Disseminating Information: Tips and how-to guides can spread through various channels—secure messaging apps, coded newsletters, or "rumor networks" in large corporations. Trained agents may directly coach willing participants, especially where face-to-face communication remains safest.

MINIMIZING RISK

Fear of Detection: The scope of sabotage often hinges on perceived risks. High-profile arrests or firings spread quickly and discourage participation.

Practical Safeguards: Teach saboteurs to use everyday items—like cleaning sprays, tape, software macros—to sabotage equipment in ways that blend into normal tasks. Encourage them to commit acts that could plausibly be blamed on "common mistakes," such as "forgetting" to refill printer paper or "accidentally" mislabelling cables in a server room.

Timing and Targets: Focus on vulnerabilities and gear sabotage toward acts unlikely to arouse suspicion, like sporadic or disguised errors. Doing so keeps suspicion low and ensures a steady rate of disruption.

CHALLENGES IN CONTROLLING CITIZEN-SABOTEURS

Because simple sabotage is performed by everyday individuals acting on their own initiative, it's almost impossible to centrally manage or synchronize these efforts with precise strategic demands. Moreover, any concerted attempt to align sabotage with major operations could tip off adversaries that significant action is imminent.

Still, sabotage guidelines should reflect local circumstances and be periodically updated. When appropriate, underground or secure channels—such as online bulletins, community-based apps, or discreet propaganda—can emphasize which general targets are most critical at a given time (e.g., data centers, major logistics hubs, or large corporate offices).

GENERAL CONDITIONS

Beyond Vandalism: Simple sabotage should always have a tangible effect on enemy or adversary operations—whether by wasting resources, time, or labor.

Creativity with Everyday Items: A saboteur who reconsiders their routine surroundings will find countless "weapons"—e.g., staples that jam printers, poorly placed network cables that create bottlenecks, or mislabeled boxes that delay shipping.

Right-Sized Targets: Avoid attempts too technical or dangerous for your skill level. Untrained individuals should not handle complicated destructive methods (e.g., advanced hacking or explosives). Stick to simpler acts, like gluing locks, messing with file permission settings, or stealthily removing lubrication from machinery.

Confirm the Usage: Make sure the resource or system you plan to sabotage is actually valuable to the target. High-grade fuels and advanced computing resources are typically crucial for an adversary. By contrast, destroying random office supplies might accomplish little unless those supplies are essential.

Prioritize Military or High-Value Assets: Even though many citizen-saboteurs rarely access purely military hardware, if you do have proximity to specialized equipment—like communication servers or security gear—those should take precedence.

BEFORE A MAJOR OFFENSIVE OR CORPORATE SHAKEUP

During relatively calm periods, sabotage that undermines industrial or supply-chain outputs can be highly effective, such as contaminating essential materials or quietly crippling manufacturing lines. Slashing the tires of a single delivery vehicle is worthwhile, but sabotaging an entire tire production run is exponentially more disruptive.

DURING ACTIVE OPERATIONS

Focus on immediate, localized effects that can disrupt real-time activities (e.g., misrouting shipments, corrupting data backups, disabling essential services). Even modest interference can shift the momentum if timed well.

Disrupt all types of transportation and communication: jam office routers, mislabel shipping containers, or physically sabotage important vehicles. Damage essential materials like fuel, spare parts, or even digital credentials (e.g., revoking access tokens or damaging key cards).

TARGETS, METHODS, AND MODERN ADAPTATIONS

It's important to identify the specific actions and likely outcomes defined by simple sabotage so that potential saboteurs understand what is feasible in a contemporary setting. Below is a detailed list of targets and tactics, updated for offices, manufacturing sites, data centers, and beyond. Consider it a living document: new technologies constantly open opportunities for innovation.

BUILDINGS AND PHYSICAL FACILITIES

Offices, hotels, warehouses, data centers, factories—these remain prime locations for simple sabotage. They frequently store critical equipment, records, or inventory, and offer plenty of ways to create damage or delay.

Fires:

Where physical documents or flammable materials are still common, small, unattended flames (started by candles, overheated electronics, or purposefully sabotaged wiring) can cause significant property damage.

In data centers, tripping or disabling fire-suppression systems (often automated with gas or foam) before initiating a small fire can lead to extensive hardware losses.

Sprinkler and Water Damage:

Triggering or tampering with sprinkler systems in offices can ruin electronics, damage files, and force a costly cleanup.

Clogging drains in kitchens, restrooms, and server-room cooling areas can create floods or water backups.

Electrical Interference:

“Shorting” circuits by inserting conductive objects (coins, paper clips, etc.) behind fuse panels can kill power in entire floors.

Miswiring or mislabeling network and power cables can create maddening troubleshooting scenarios.

Lock Jamming and Vandalism:

Glue or jam locks on storerooms, server racks, or essential office doors. Even a modest jam can create big bottlenecks if it denies access to critical resources or data.

INDUSTRIAL MANUFACTURING AND WORKSHOPS

Although many modern economies rely heavily on service and software industries, physical manufacturing plants, construction sites, and specialized workshops still represent huge segments of production.

Tools:

Let cutting edges or blades go dull; calibrate machinery incorrectly so that parts come out off-spec.

For pneumatic or electric tools, allow dust and debris to accumulate in air intakes or lubrication points.

Oil, Lubrication, and Cooling Systems:

Introduce sand, metal filings, or even small plastic bits that can bypass filters. This leads to friction, wear, and eventual machinery failure.

Diluting or contaminating oil supplies in storage can silently degrade production quality, requiring expensive rework and repairs.

Fuel Tanks and Combustion Engines:

Adding sugar, honey, or other thick substances into fuel disrupts engines, from forklifts to backup generators.

Water, saltwater, or any non-combustible liquid also causes stalling or permanent engine damage.

Electric Motors and Transformers:

Overloading or miscalibrating motors leads to overheating or breakdown.

For large transformers or power systems, blocking ventilation or introducing conductive dust can trigger short circuits.

MINING, AGRICULTURE, AND RESOURCE EXTRACTION

While technology might have evolved, basic sabotage methods in large extraction industries still apply:

Mining:

Disrupting conveyor belts or cart tracks, adding rocks to high-value mineral loads, or contaminating coolants in pneumatic drills.

Slowly weakening chains or rail connections so they break under normal load, causing downtime.

Agriculture:

In areas where the adversary relies on food production, mismanagement of harvest scheduling, water, or storage can spoil large portions of crops.

Overwatering, failing to protect stored grains from pests, or mixing damaged goods with healthy produce can cause rapid declines in usable food.

TRANSPORTATION AND LOGISTICS (RAIL, ROAD, WATER, AND AIR)

Rail:

Mislabeling cargo, swapping signals, placing minor obstructions on tracks, or loosening rail ties can cause delays or derailments.

Modern train systems rely heavily on digital signals; introducing system errors or misconfiguring track software is equally potent.

Road:

Removing or altering road signs, spreading nails or glass to puncture tires, and giving false directions significantly slows shipments.

In an IT-sense, if route-planning software or GPS systems can be hacked or misconfigured, entire fleets can be rerouted incorrectly.

Waterways:

Barge pilots and port workers can add to transit times with "accidental" groundings, misinformation about channel depth, or incorrect cargo manifests.

Digital shipping records can be subtly corrupted so cargo is lost, delayed, or delivered to the wrong location.

Aviation:

While not in the original text, modern sabotage includes misrouting baggage, misfiling flight plans, introducing small hardware or software errors in critical systems, or draining resources needed for safe operation.

COMMUNICATIONS AND IT

Modern organizations depend on reliable digital and analog communications—making these systems excellent sabotage targets.

Telephones and VoIP:

Misdirect calls, drop lines “accidentally,” reroute voice traffic through slow or overloaded links, or remove essential hardware from phone systems.

Email and Messaging:

Divert urgent messages into spam folders, corrupt attachments, or rename files to sow confusion.

Overwhelm chat channels with trivial or redundant posts, burying important information.

Overuse the “Reply All” feature in email chains. This will clog mailboxes with useless messages and potentially bury important emails among junk.

Network and Internet:

Physically unplug or swap cables in server rooms, cause IP conflicts, or introduce deliberate misconfigurations in routers and firewalls.

Exploit known software vulnerabilities to cause intermittent outages or degrade system performance.

Introduce inefficiencies in company networks by overloading them with unnecessary data or running resource-intensive processes in the background. This will slow down operations and frustrate employees.

Software & Development

Encourage rewriting code unnecessarily – Argue that it needs to be "modernized" even if it works fine.

Insist that every task needs a formal process – Even for things that should be quick.

Push for frequent reorganization of teams so no one has time to settle into a workflow.

Physical Mail Services:

Misaddress or reorder physical mail, especially if critical documents must be in paper form. Delay or lose time-sensitive packages.

Media and Propaganda:

Overmodulate or jam broadcast signals. In digital streaming or recorded announcements, add background noise or hamper audio quality.

Use well-placed disruptions during remote conferences or corporate events, such as "accidental" screen-sharing of irrelevant or off-topic material, to undermine official narratives.

POWER AND DATA CENTERS

Modern enterprise depends on reliable power and uninterrupted data. These are particularly high-value sabotage points.

Power Generation and Distribution:

Subtly disable or degrade turbines, generators, or large battery backups. Introduce inefficiencies that drain energy.

Technicians can miswire connections, remove insulation from cables, or tamper with transformers to create localized blackouts or brownouts.

Data Centers and Server Infrastructure:

Overheat equipment by disabling cooling or partially blocking vents in server racks.

Tamper with uninterruptible power supplies (UPS) so that servers crash during even minor power fluctuations.

Re-label cables and devices to confuse IT staff, causing hours of diagnosis for a simple fix.

ORGANIZATIONAL AND ADMINISTRATIVE INTERFERENCE

Not all sabotage needs to be physical. Organizational sabotage relies on bureaucracy, miscommunication, and wasted effort to slow productivity.

Meetings and Decision-Making:

Insist on formal procedures for trivial matters, convene large committees, and question every detail to delay decisions.

Revive previously settled issues repeatedly, wasting time and creating frustration.

Managers and Supervisors:

Request written instructions for every single task, then claim misunderstanding or ask endless clarifying questions.

Assign critical tasks to unqualified staff while giving skilled employees trivial, morale-sapping projects.

Office Personnel:

Make data entry errors, misfile digital documents, or lose track of essential attachments in email threads.

Tell important callers that your manager is busy or redirect them to incorrect contacts. Delay or ignore follow-ups.

General Employee Tactics:

Work slowly, add unnecessary steps to processes, and pretend confusion over routine tasks.

Blame bad tools or out-of-date software for consistent underperformance.

Mismatch or mix good items with broken or flawed items in inventory systems.

LOWERING MORALE AND SPREADING CONFUSION

Finally, sabotage can include subtle actions designed to degrade morale and trust:

Disruptive Behavior:

Give overly technical or irrelevant answers to simple questions.

Spread rumors about impending layoffs, policy changes, or operational failures that sound plausible but lack evidence.

In workplaces with smart technology, tamper with thermostats, lighting systems, or other IoT devices to create discomfort.

Social Cold-Shoulders and Symbolic Resistance:

End conversations when certain managers or “enforcer” figures enter a room.

Publicly avoid or boycott company-sponsored events or messages from undesired authorities.

Emotional Displays:

Overreact or cry on small provocations, pressuring management or local authorities to handle every minor situation gently, slowing their response to real issues.

Bureaucratic Entanglements:

Insist on “proper procedure” for trivial tasks—like forms, approval processes, or scheduled times—even in emergencies.

Non-Cooperation in Alleged “Civic” or “Patriotic” Programs:

Avoid or undermine official philanthropic or volunteer campaigns if they primarily serve an oppressive entity.

Quietly discourage participation by pointing out inefficiencies or suspect uses of the funds.

NOTES

MONODON PRESS