# Data Destruction Method – SSD in Military Applications

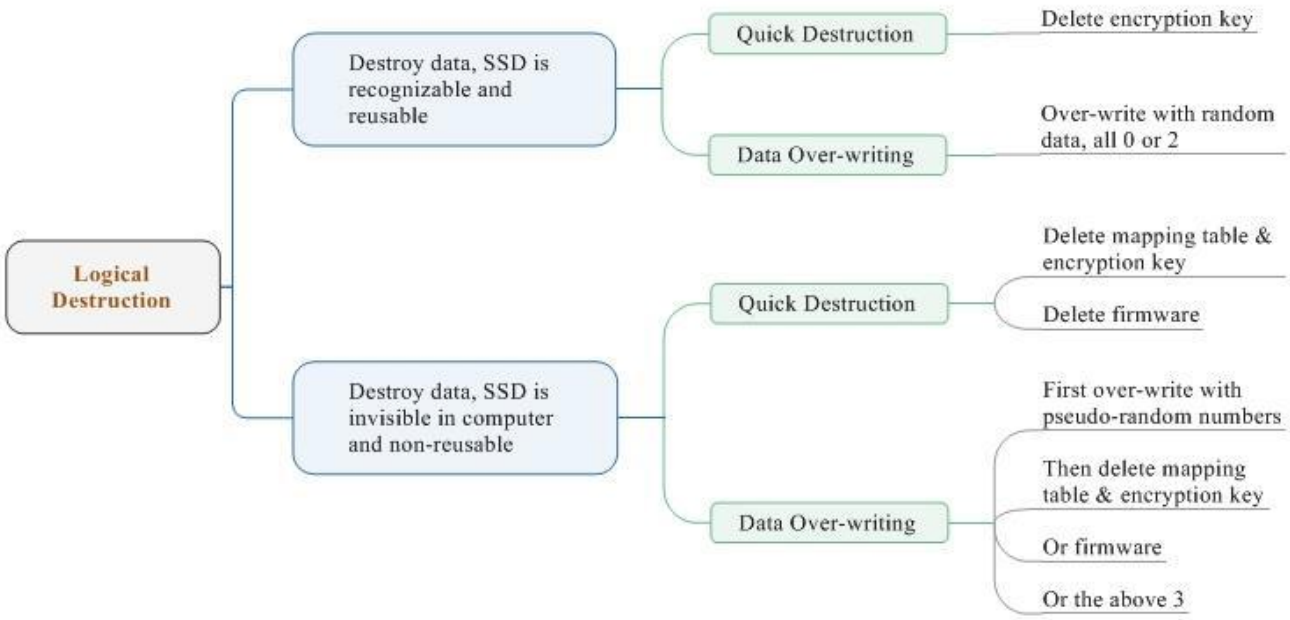
For military applications, data security concerns military secrets or even decides the outcome of the war. Especially in modern warfare, on the one hand, countries go all out to develop more advanced and safer electronic systems, and on the other hand, they try every means to decode each other's systems. And yet, as the data medium, the hard disks try all encryption methods to prevent being decrypted and meanwhile pay closely attention to quick erase or data destruction under various emergency environments.

## Data Destruction Classification

In general, data destruction is divided into two types:

One is Logical Destruction which only destroys the data but not the physical chipsets. SSD is reusable after data-destructing or firmware re-implanting.

Logical Destruction normally executed by two mode: ① Quick Destruction (namely fast purge), to delete the data information quickly by pressing erase key; ② Data over-writing or filling which usually takes several hours depending on the SSD capacity. These data destruction methods can be implemented by software, but mostly by hardware.




Generally Quick Erase is not actually erasing data, thus it is risky at some level, but it is inevitable and important under urgent environment.

Another type is Physical Destruction with chipsets inside burned directly, that the data recovery is impossible in this way.

Physical Destruction generally utilizes the following methods: crushed by hammer or other heavy stuff, destructed by strong acid, destroyed by explosive or burned the chipsets by high voltage.

## Approaches for Data Destruction

In general, both logical and physical data destruction can be implemented through specified Pin or a hardware key if the host system and SSD device unify the Pin definition.

It is necessary to set misoperation time for the destruction through hardware key, normally a few seconds before triggering the destruction function.

Physical destruction by high voltage is much more difficult than logical destruction, and the more difficult part is how to ensure every piece of NAND Flash chipsets being burned up. Theoretically, it can be easily realized by several methods to burn the chipsets one by one, while in view of practice, burning up one chipset usually takes long time and may not continue burning the next chipset thereafter or maybe there's some chipsets failed to be burned up.

## Destruction Standards

The data destruction standard is different from each country. Some require over-writing for 7 times while some others require for 4 times, and some countries regard deleting the encryption key as secure destruction. The security department in each country has different requirements for data destruction standards and methods, so just implement corresponding mechanism for SSD solutions.

Application Scenarios

### I.Acceleration Sensing Physical Destruction SSD

This is an application in warcraft, the design purpose is to prevent military data leakage when the warcraft is shot down. To solve the data destruction in this case, the accelerometer could be inserted in SSD. When the craft start falling down, it would sense the acceleration and trigger the data destruction automatically when reaching the present threshold value to destruct the SSD physically. No need manual operation during the whole process. Even if the crashed warcraft is found, the internal military data information has vanished.

### II.Remote Destruction

Remote Destruction is getting pretty common, even iPhone supprots remote data destruction and many SSD solutions also utilize a SIM card internally to implement the remote destruction function. Therefore the data destruction by methods of sending messages is quite "low" among present technologies.

For military applications especially outdoor ones, utilizing GPS (e.g. BeiDou in China) can also realize remote positioning and destruction, and more reliable. It requires authorization to usa GPS, navigation system is usually one-way communication which can only receive satellite signal but not send signal to satellite, the military can execute remote destruction through satellite after getting authorized.

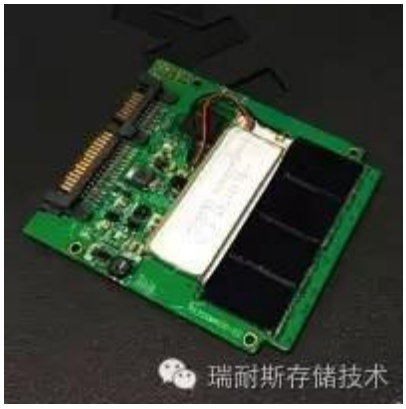
Whether GPS or SIM Card, they have to solve the signal problem.

**III.Automatic Destruction when leaving the specified location**

Restrict the use of the disk in a certain area (e.g. inside the Command Post), the destruction program will start automatically when the computer is detected leaving out of the distance of the specified location.

**IV.Physical Destruction continues after external Power Supply being cut off**

When the external power supply is cut off during executing data destruction, SSD will continue to finish the process using the reserved power offered by built-in batteries or capacitors.




**V.Unfinished Destruction continues after Retry Powering on the disk when the external power supply is cut off during the data destruction process, the destruction will be stopped, but it will continue the unfinished part after retrying powering on the SSD.**

The disadvantage for this method is that there is a potential risk for the un-destructed data to be recovered if the enemy decodes data through disassembling the NAND Flash chips.

**VI.Re-define Pin Assignment, SSD starts to destruct when connecting to a new device after leaving the original device**

The SSD is bounded together with the client's hardware, thus the SSD is irregular, and it will be burned when connected to other devices for decoding data if the enemy does't know the pin definition.