DieHarder: Securing the Heap

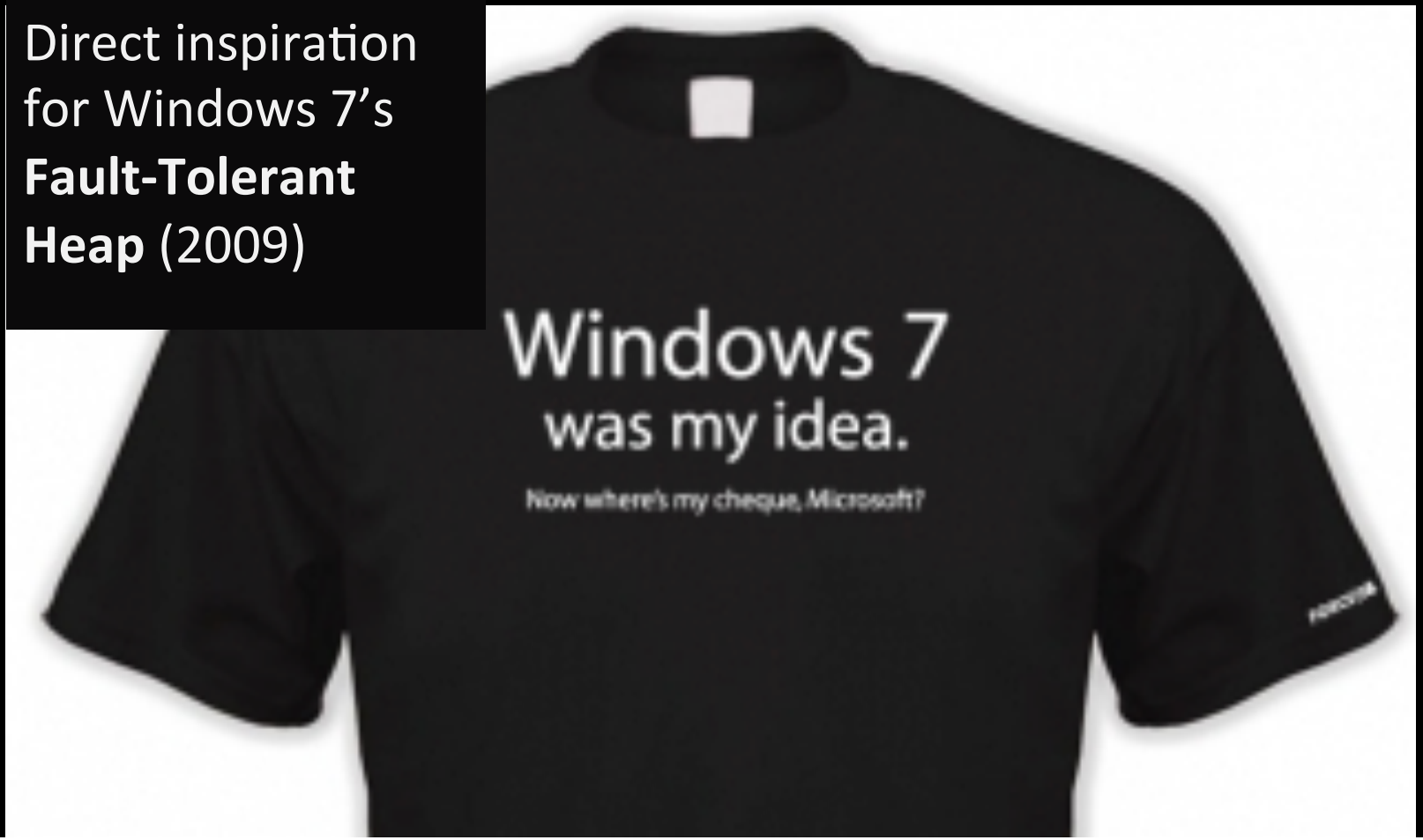
Gene Novark & **Emery Berger**

University of Massachusetts, Amherst

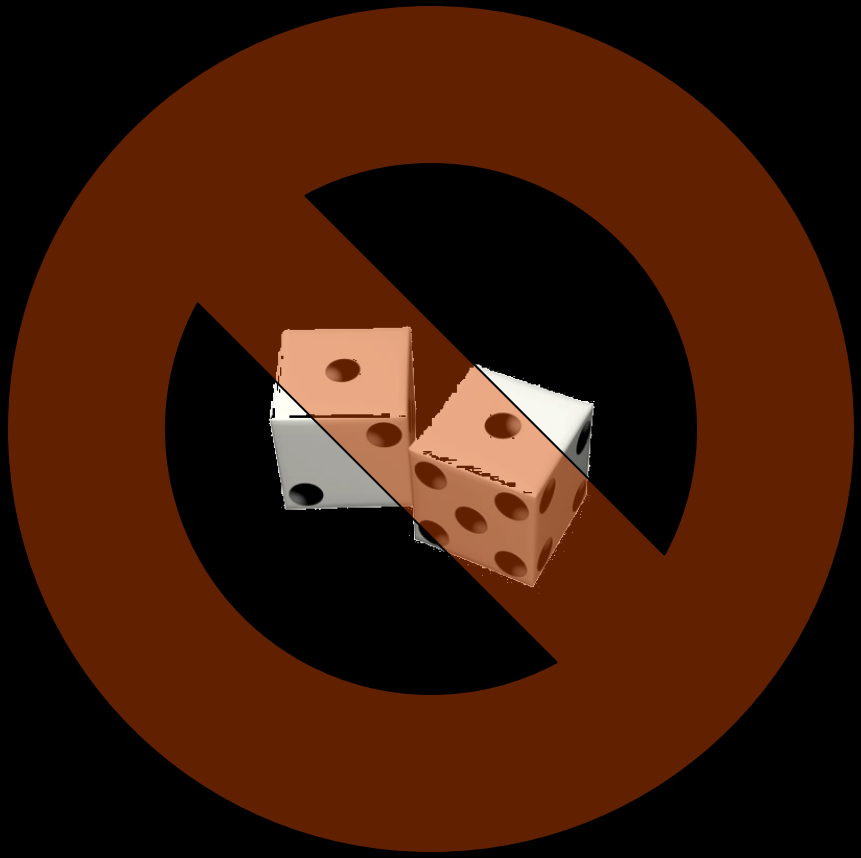
[originally presented at CCS 2011]

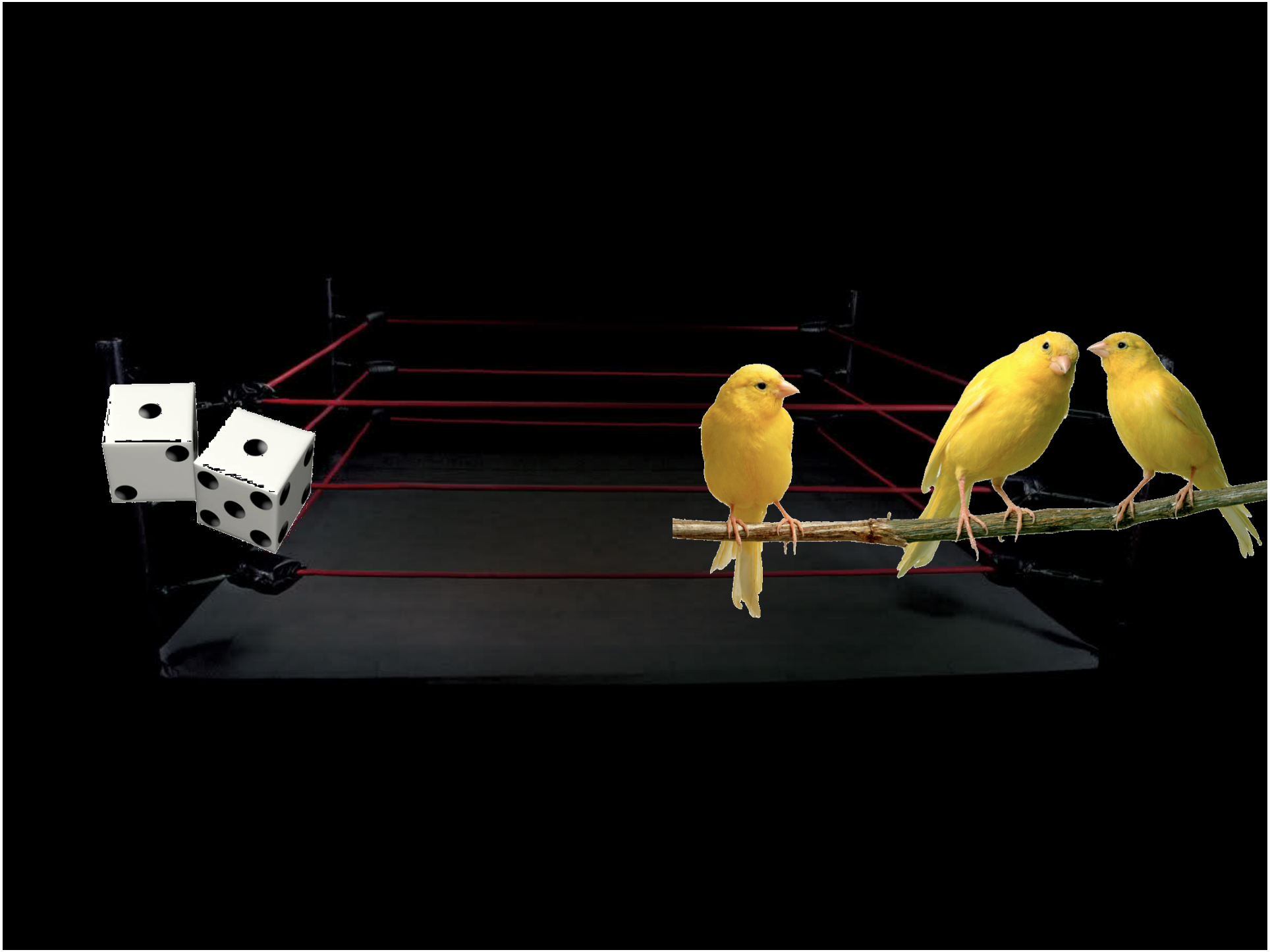
DieHard: Probabilistic Memory Safety for C/C++ Programs [PLDI 2005]

Direct inspiration for Windows 7's **Fault-Tolerant Heap** (2009)



DieHard: Probabilistic Memory Safety for C/C++ Programs [PLDI 2005]

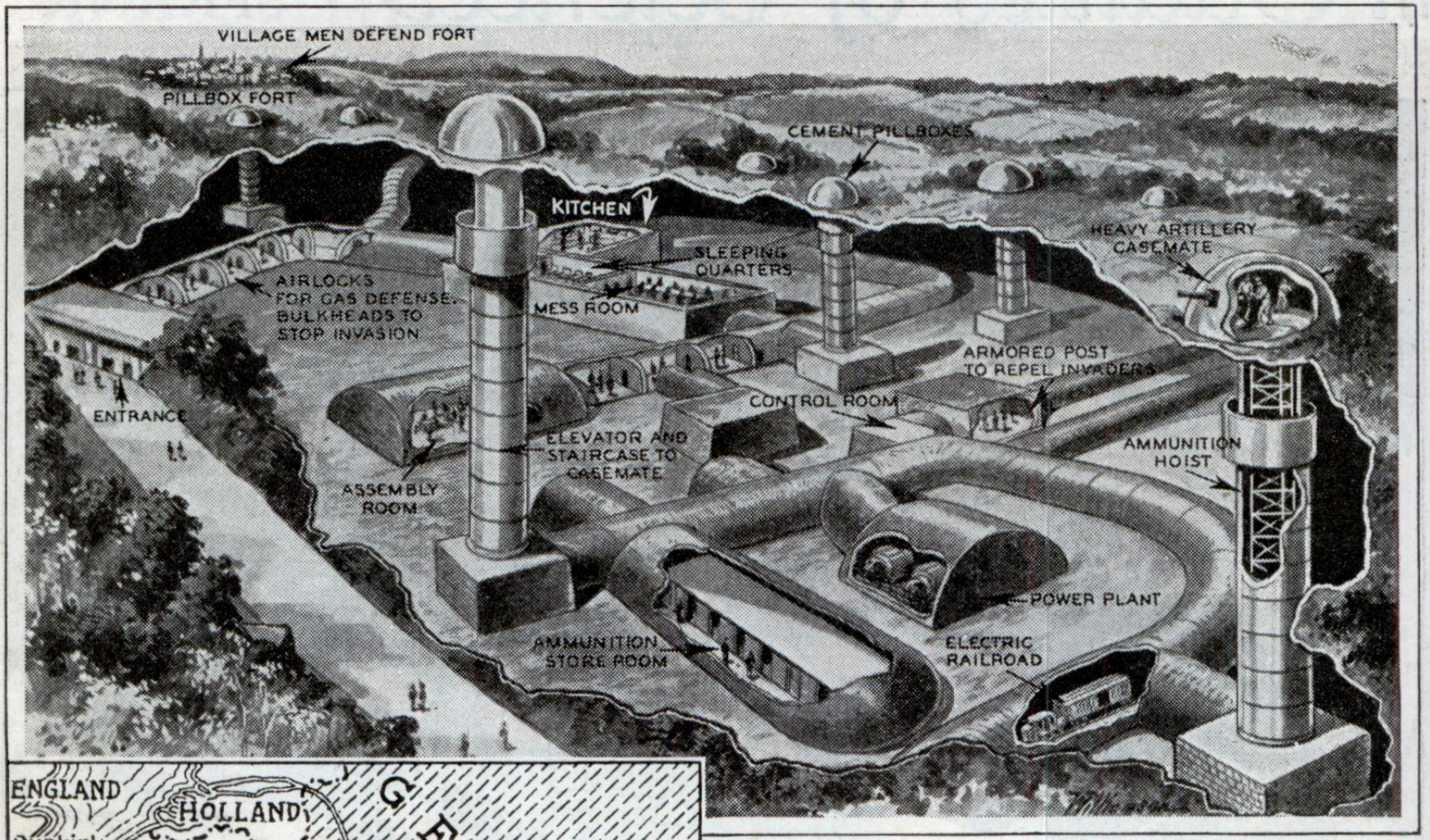


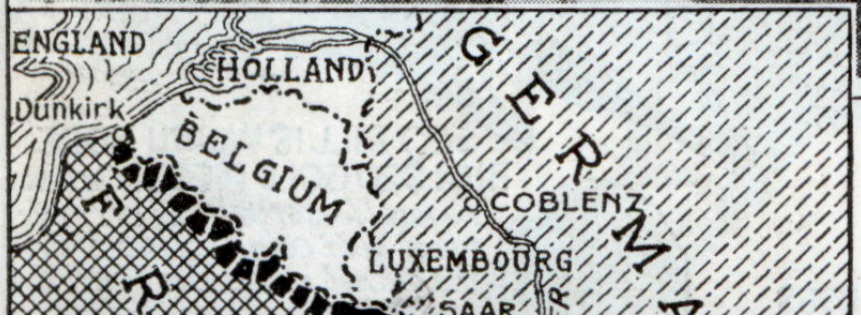



Berlin
Germany
Paris
France


Berlin
Germany

World's Greatest Underground Fortifications Guard France

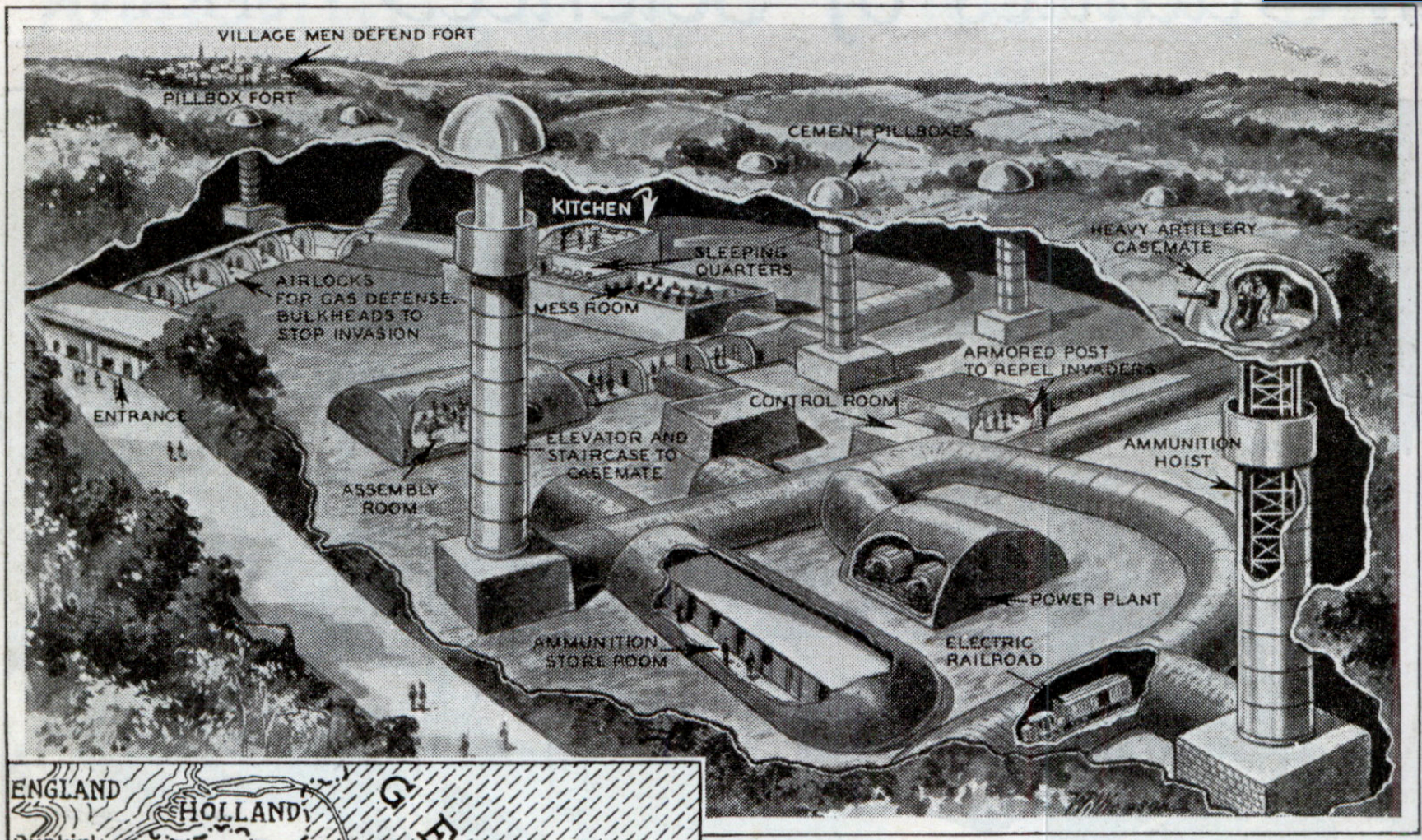


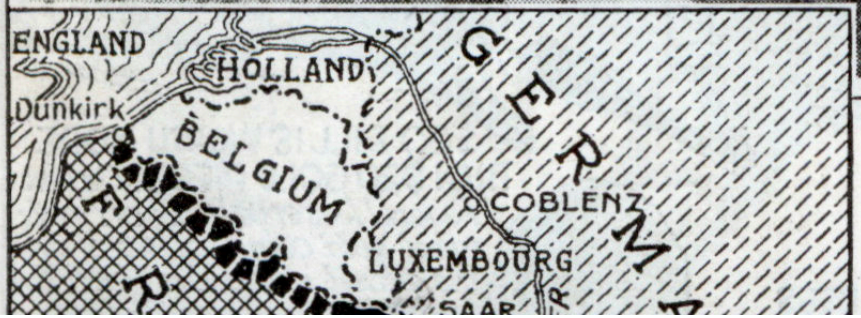


Buried deep beneath hills are the impregnable forts shown in the above drawing. Even railways are provided for.

INVISIBLE and sunk beneath the rolling and wooded terrain in Lorraine is a great underground fortification system, 200 miles

World's Greatest Underground Fortifications Guard





Buried deep beneath hills are the impregnable forts shown in the above drawing. Even railways are provided for.

INVISIBLE and sunk beneath the rolling and wooded terrain in Lorraine is a great

Solid black line shows location of 200 mile system of French underground forts, opposite disputed Saar basin.

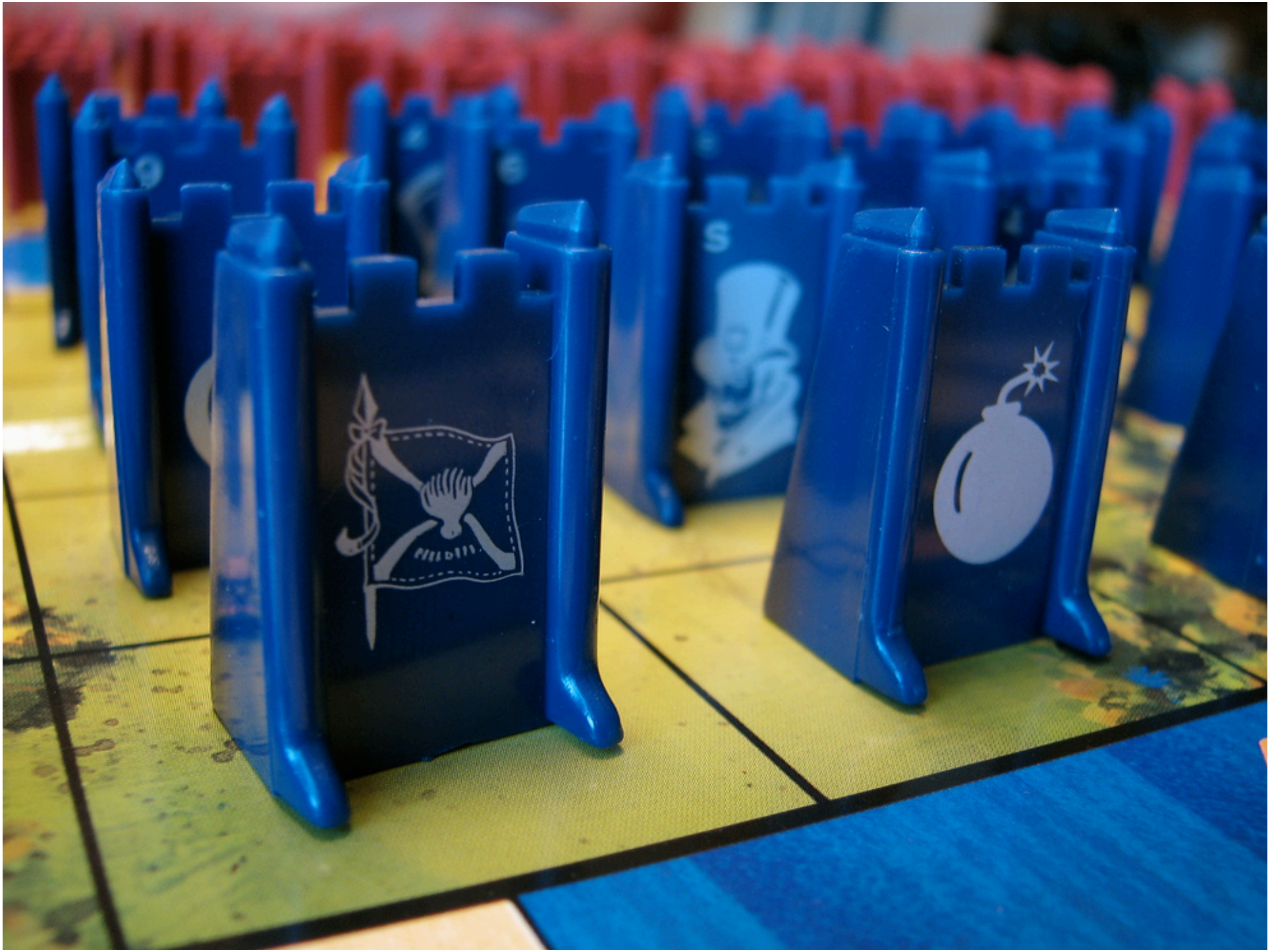
Solid black line shows location of 200 mile system of French underground forts, opposite disputed Saar basin.

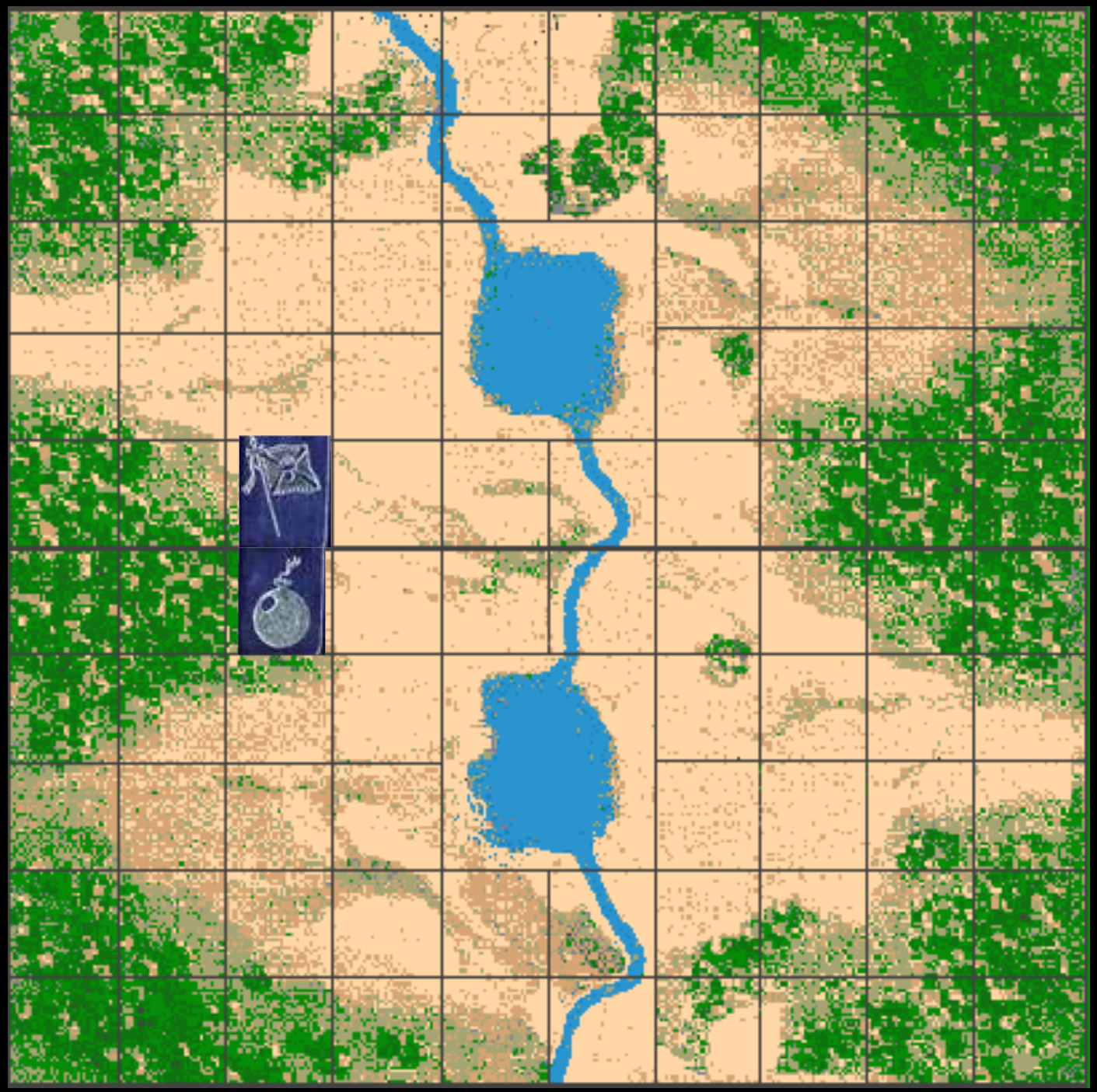
THE HEAP

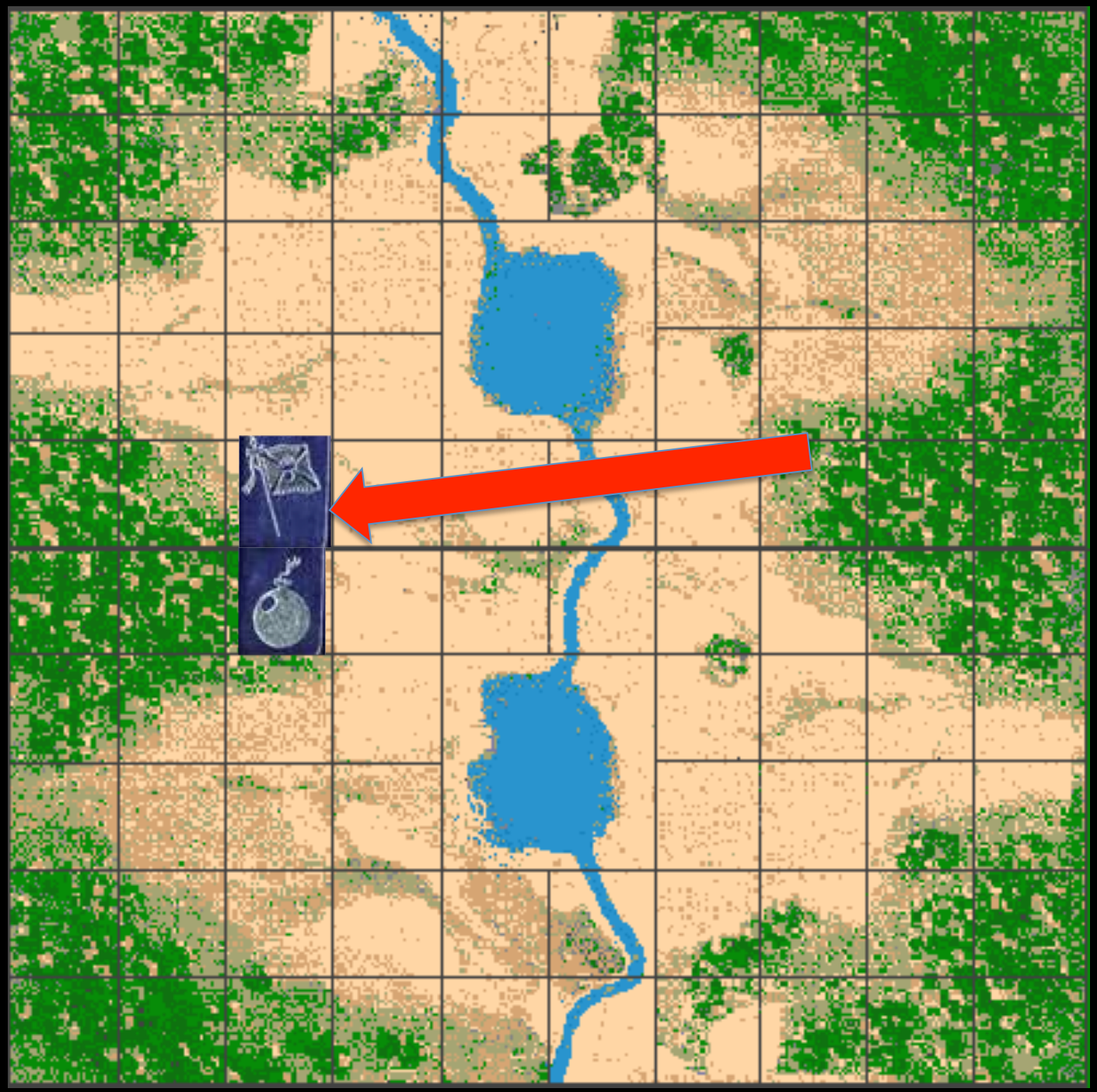
THE HEAP IS NEITHER ANIMAL NOR MAN — BUT A HALF-WORLD CREATURE THAT IS A SAD PRODUCT OF WORLD WAR #1, WHEN THE BODY OF A HALF-DEAD GERMAN FLIER, BARON VON EMMELMAN, UNITED ITSELF WITH SWAMP VEGETATION..... AND IN THE PROCESS WAS CREATED THIS PLANT-LIKE THING THAT HAS THE POWER TO REMEMBER — IF NOT TO THINK VERY EFFICIENTLY..... AND NOW.....

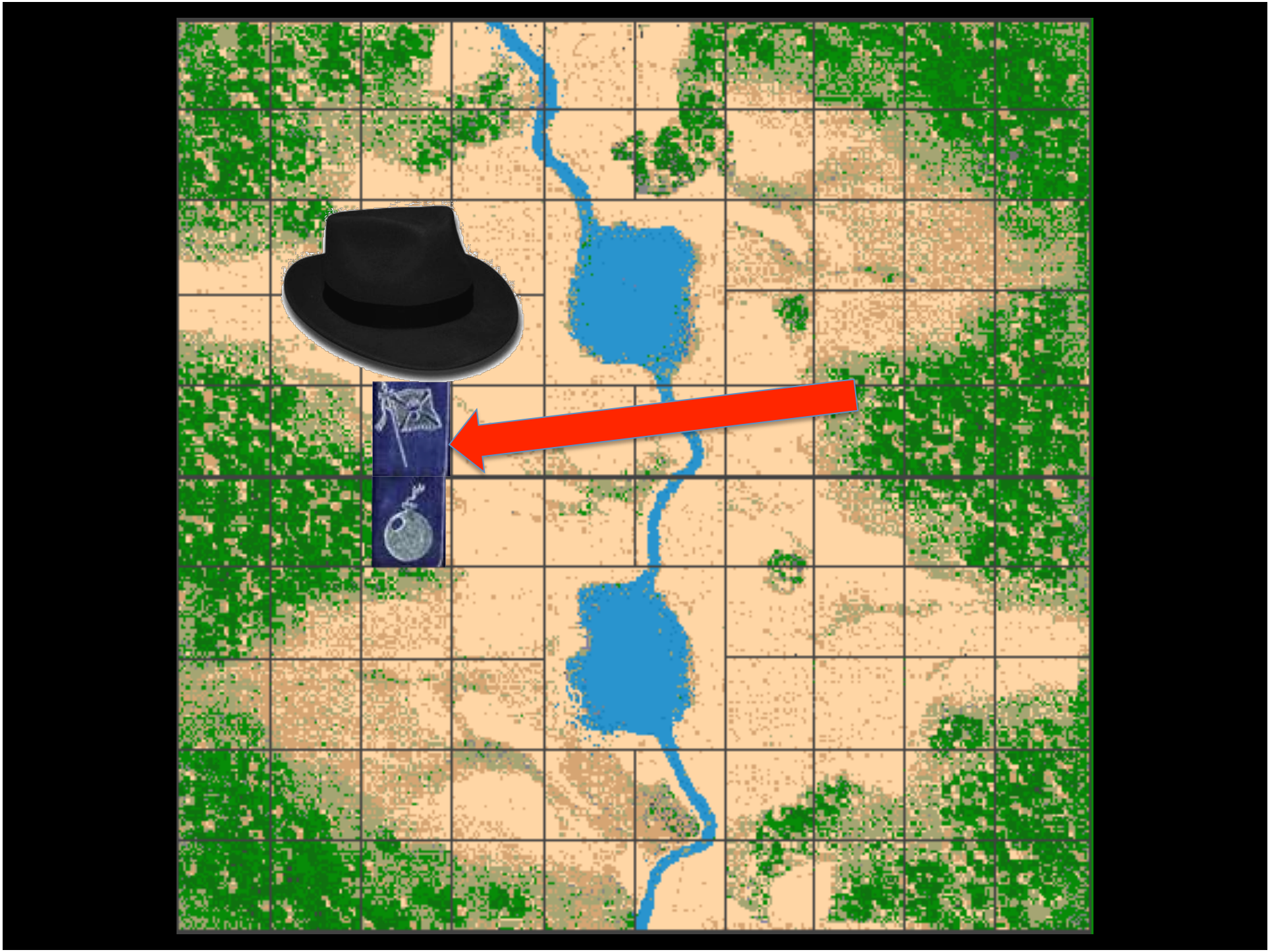

stratego
fascinating two-handed
strategy game
MB
Ages
10-Adult
2 Players
MILTON
BRADLEY
Company
START

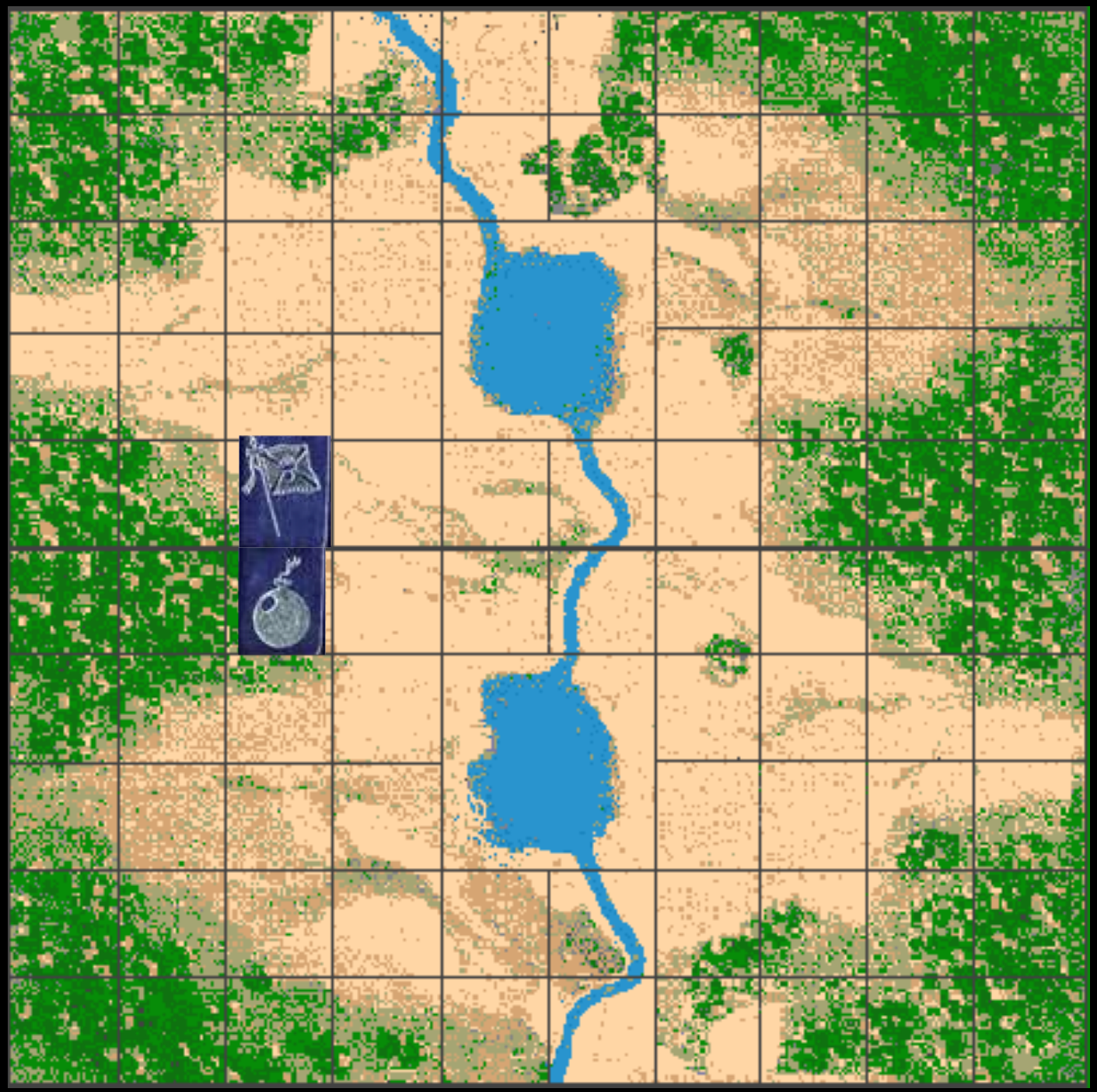

STRATEGO

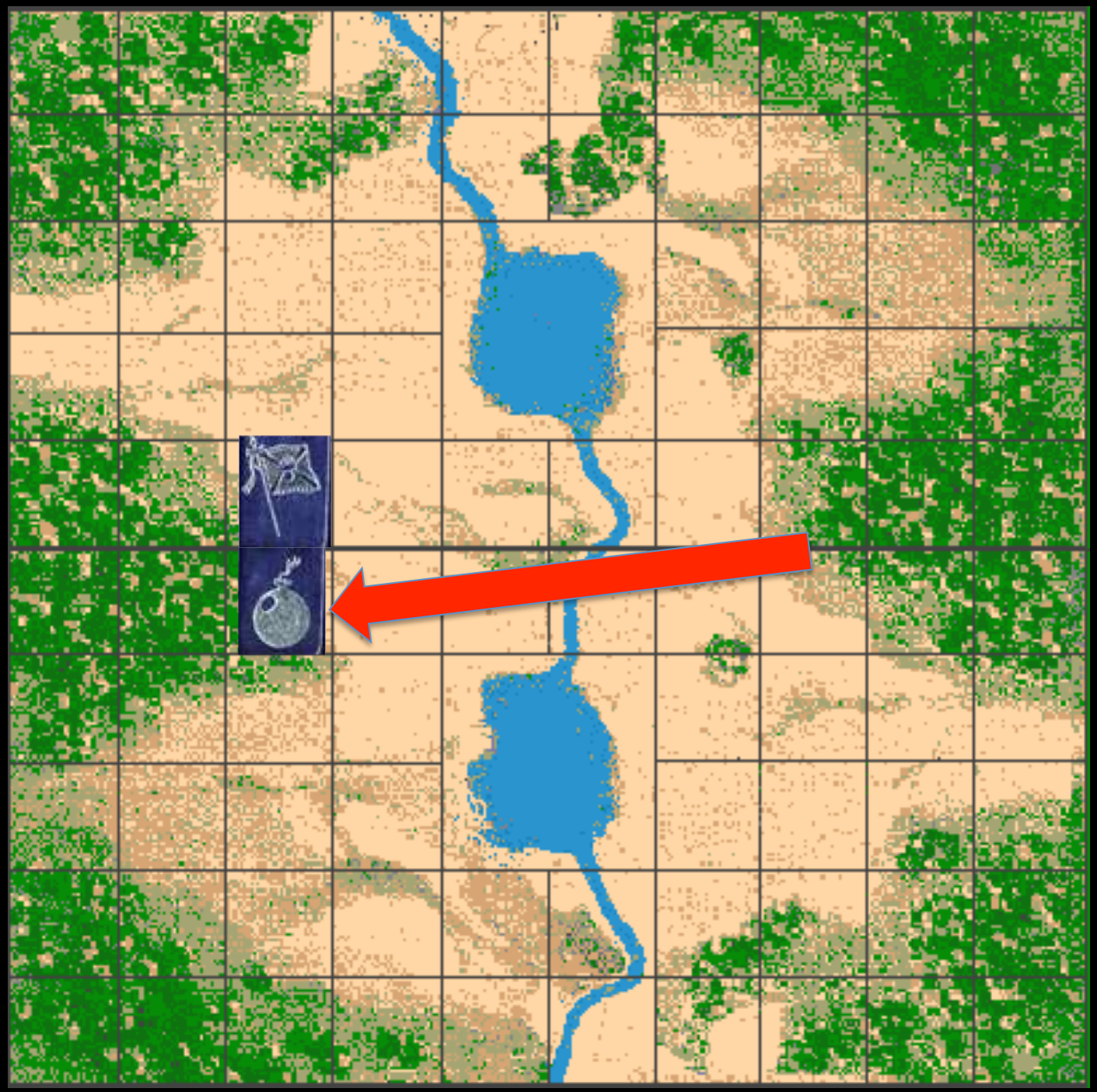


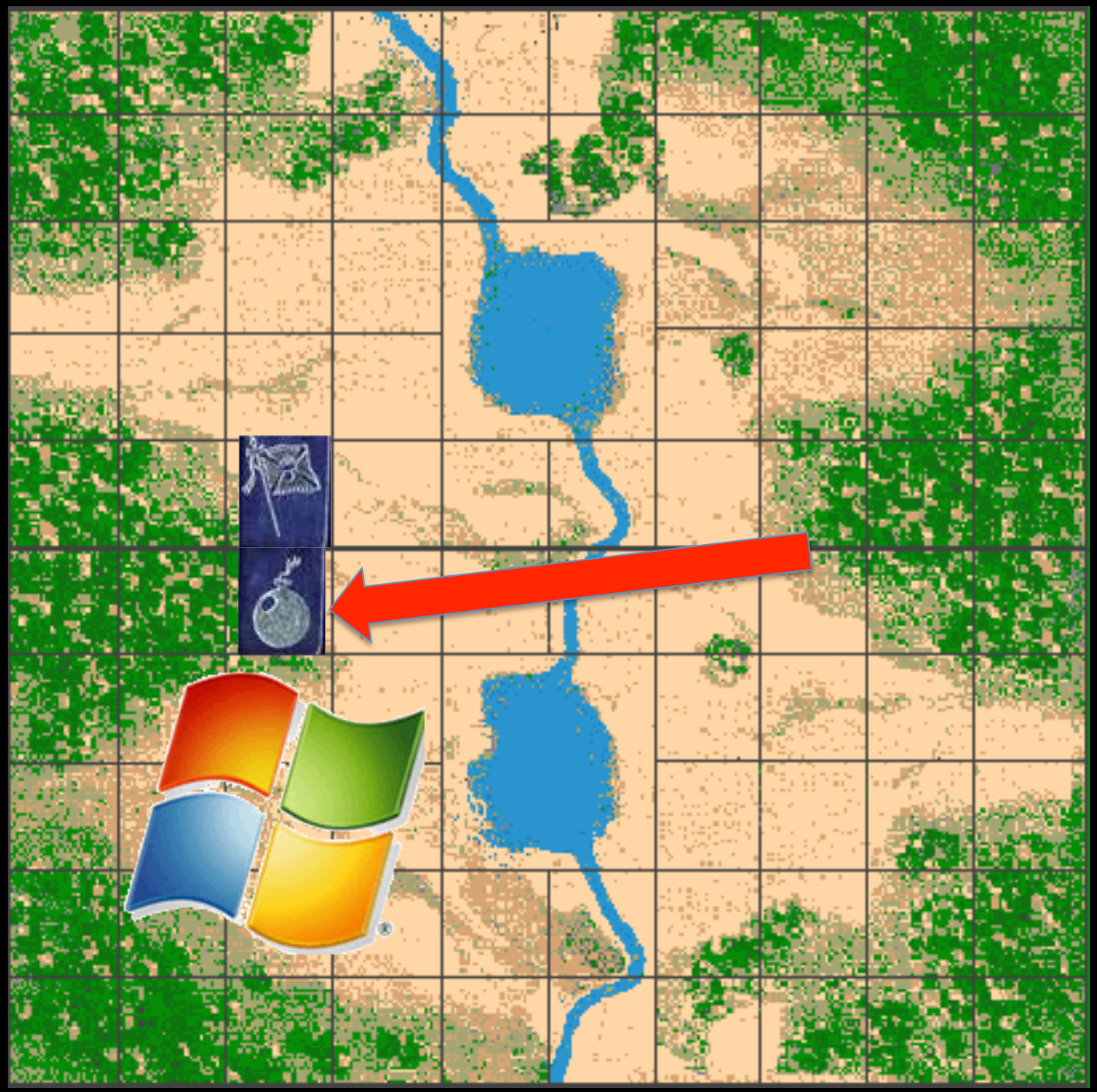


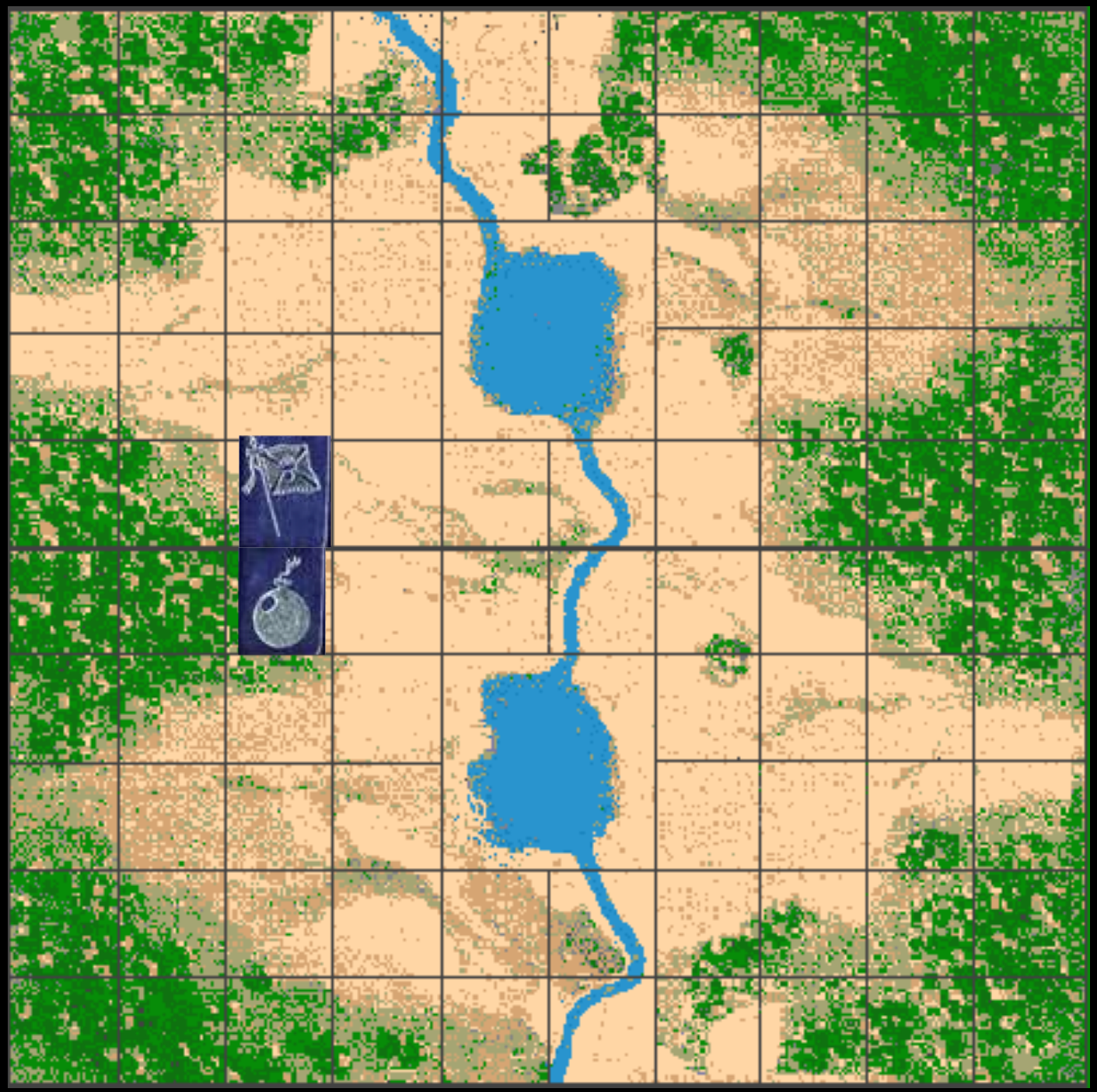




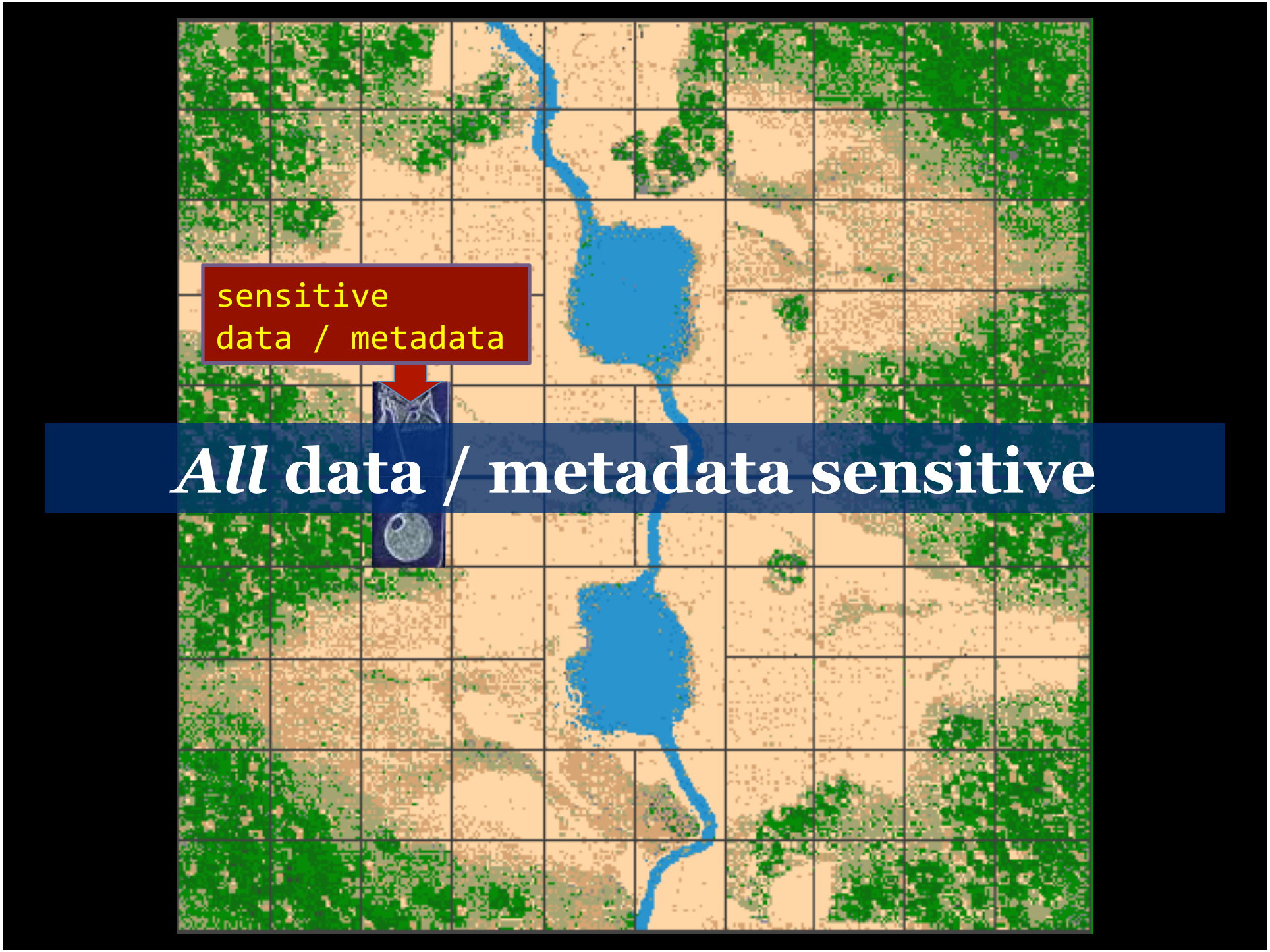


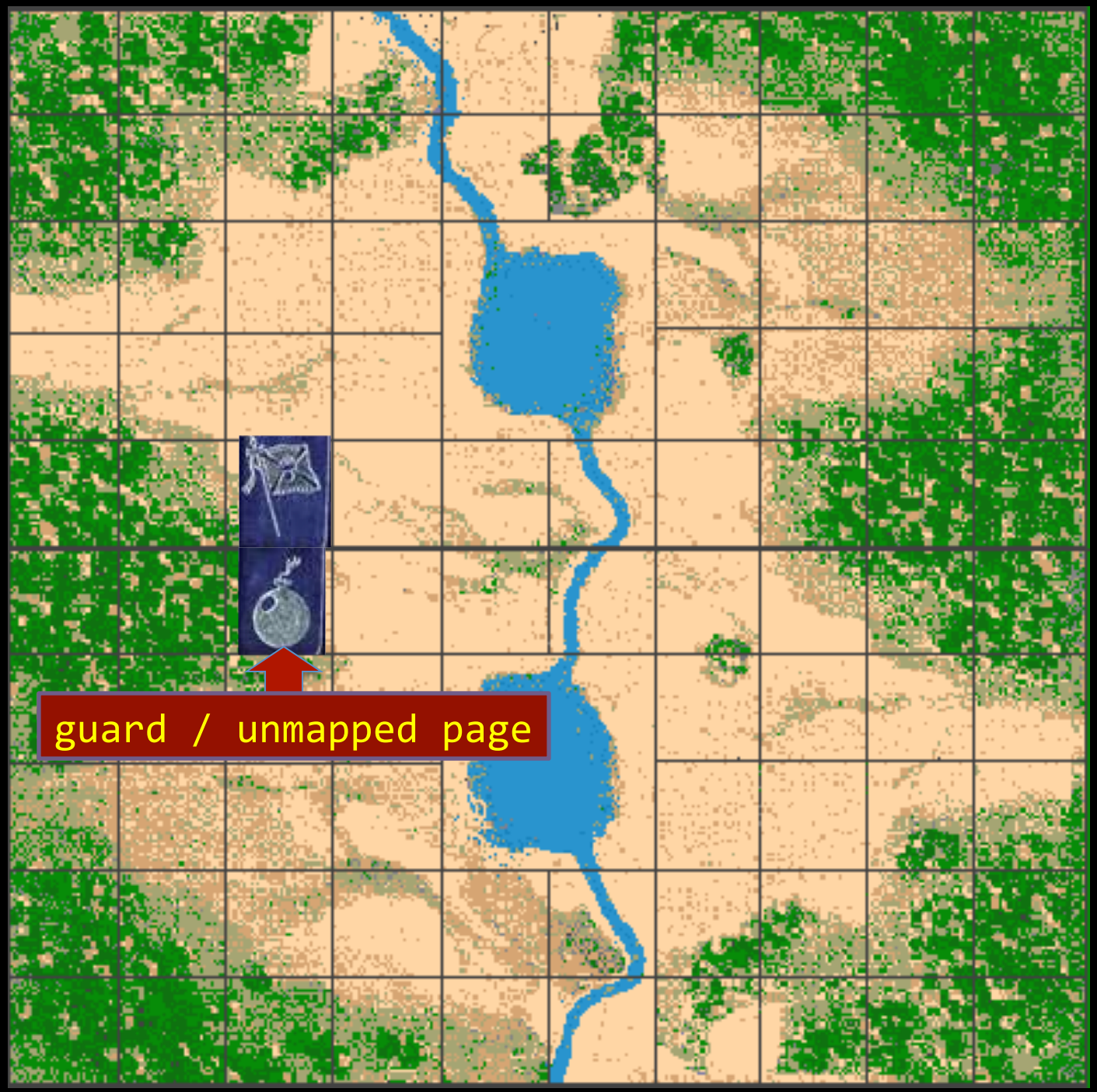


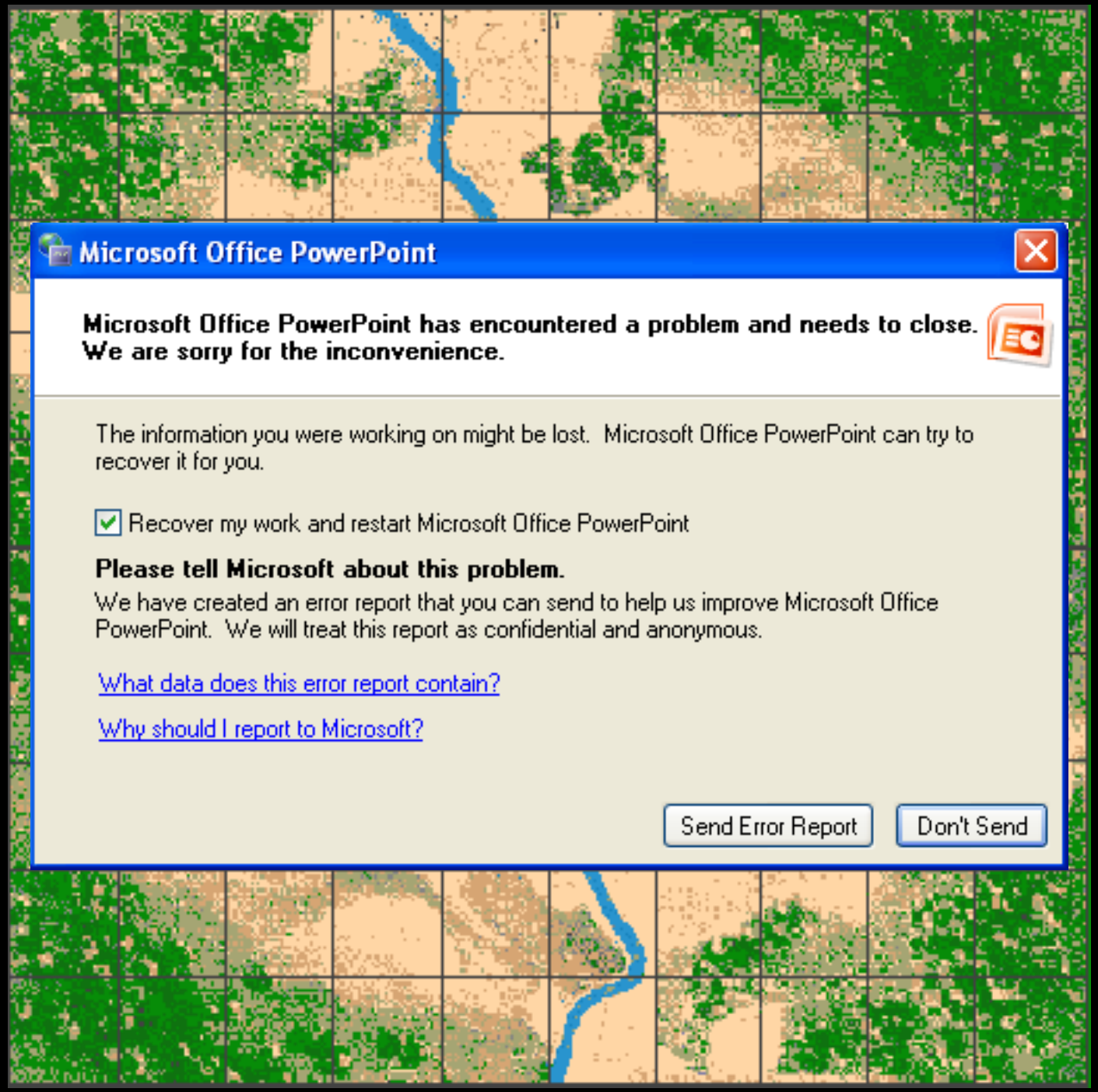


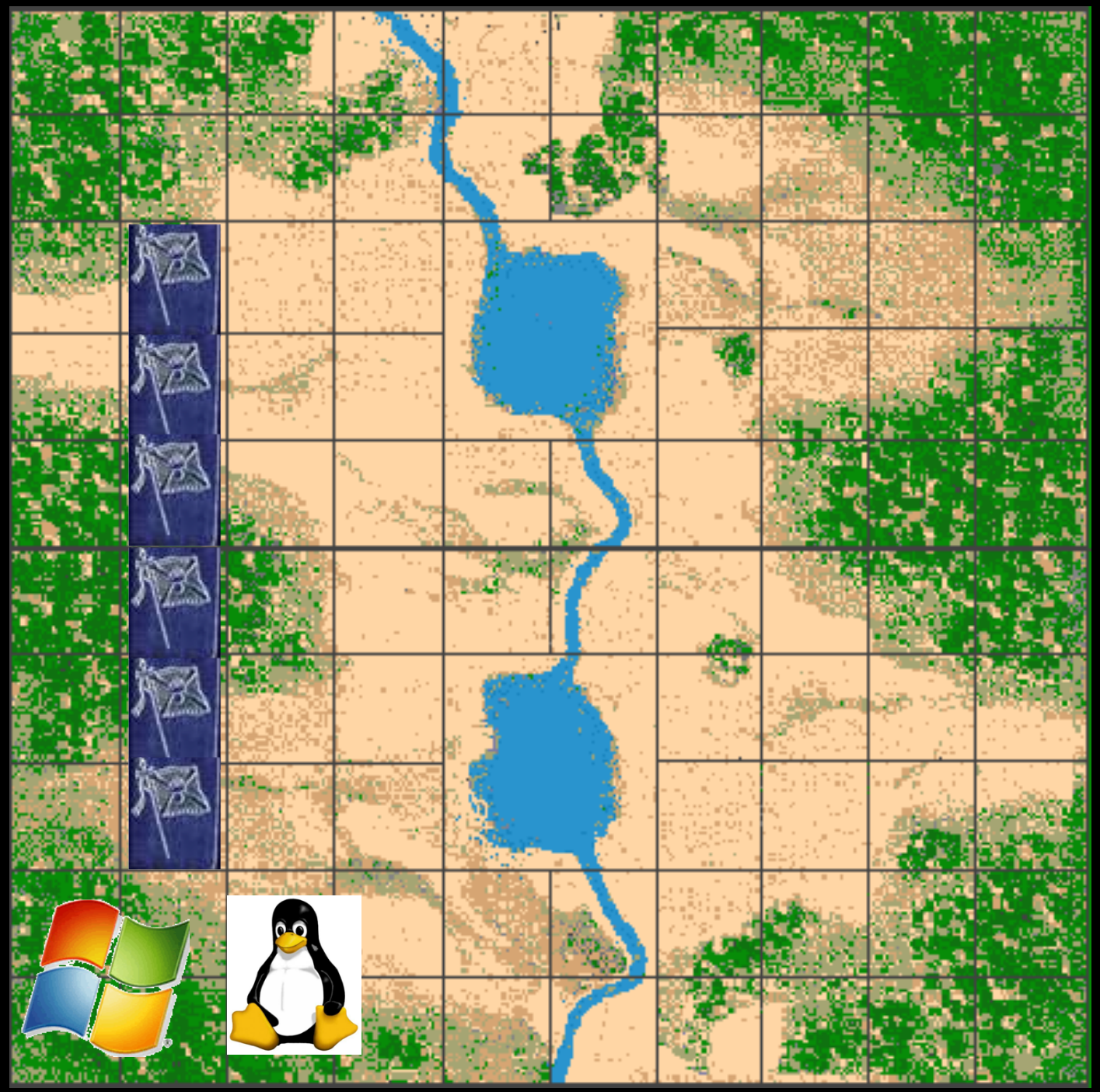


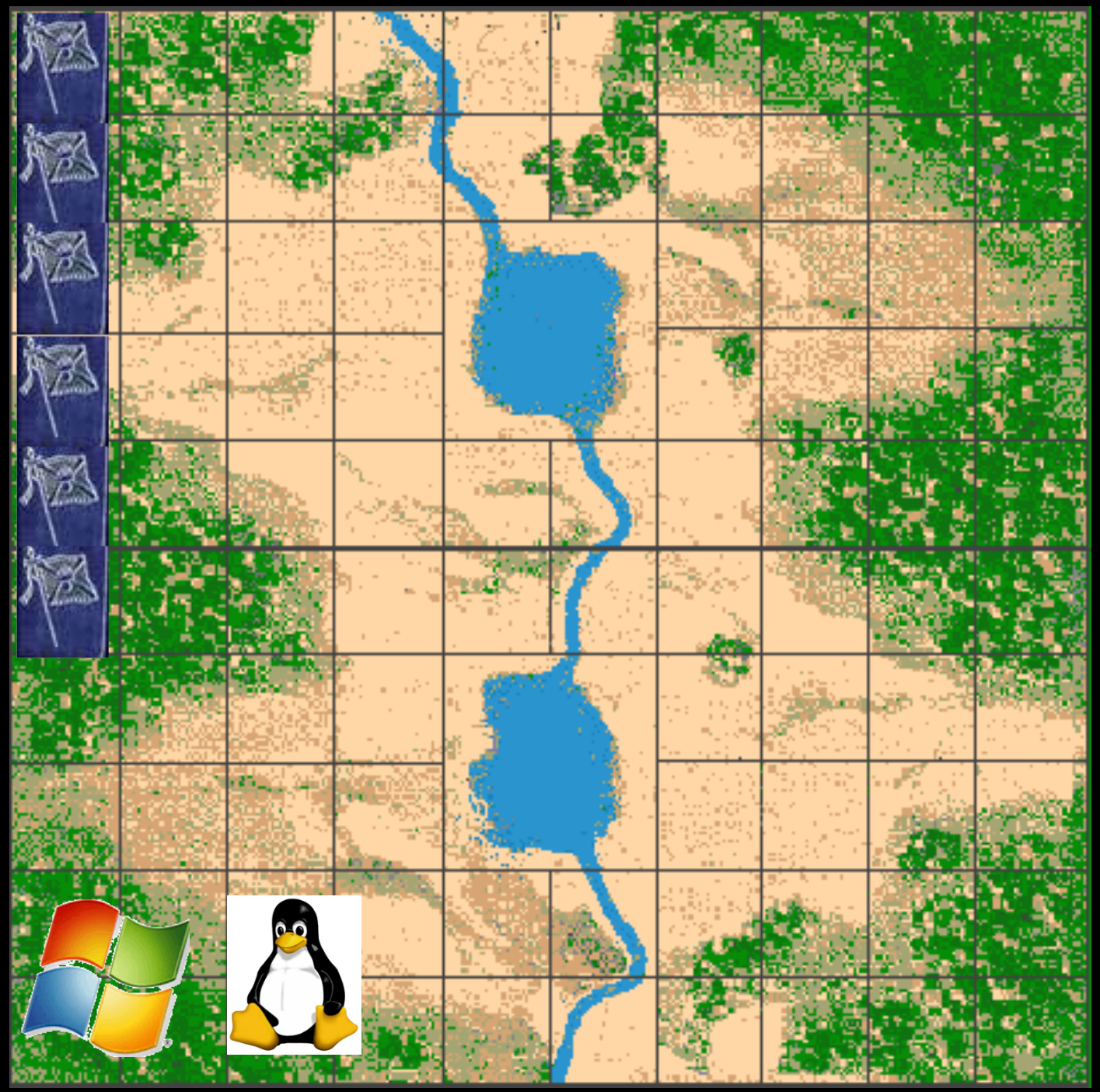

sensitive
data / metadata

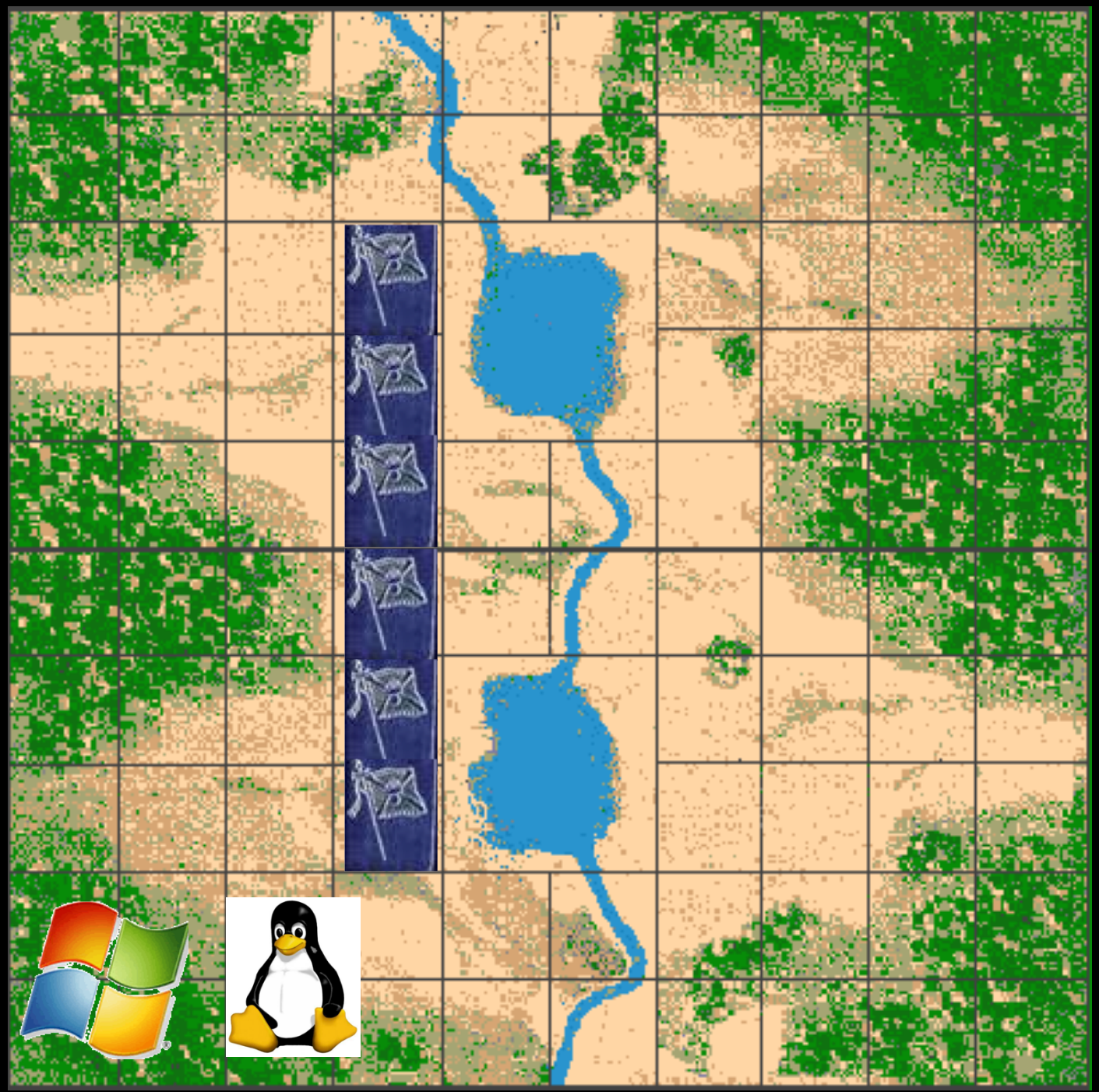

sensitive
data / metadata
All data / metadata sensitive

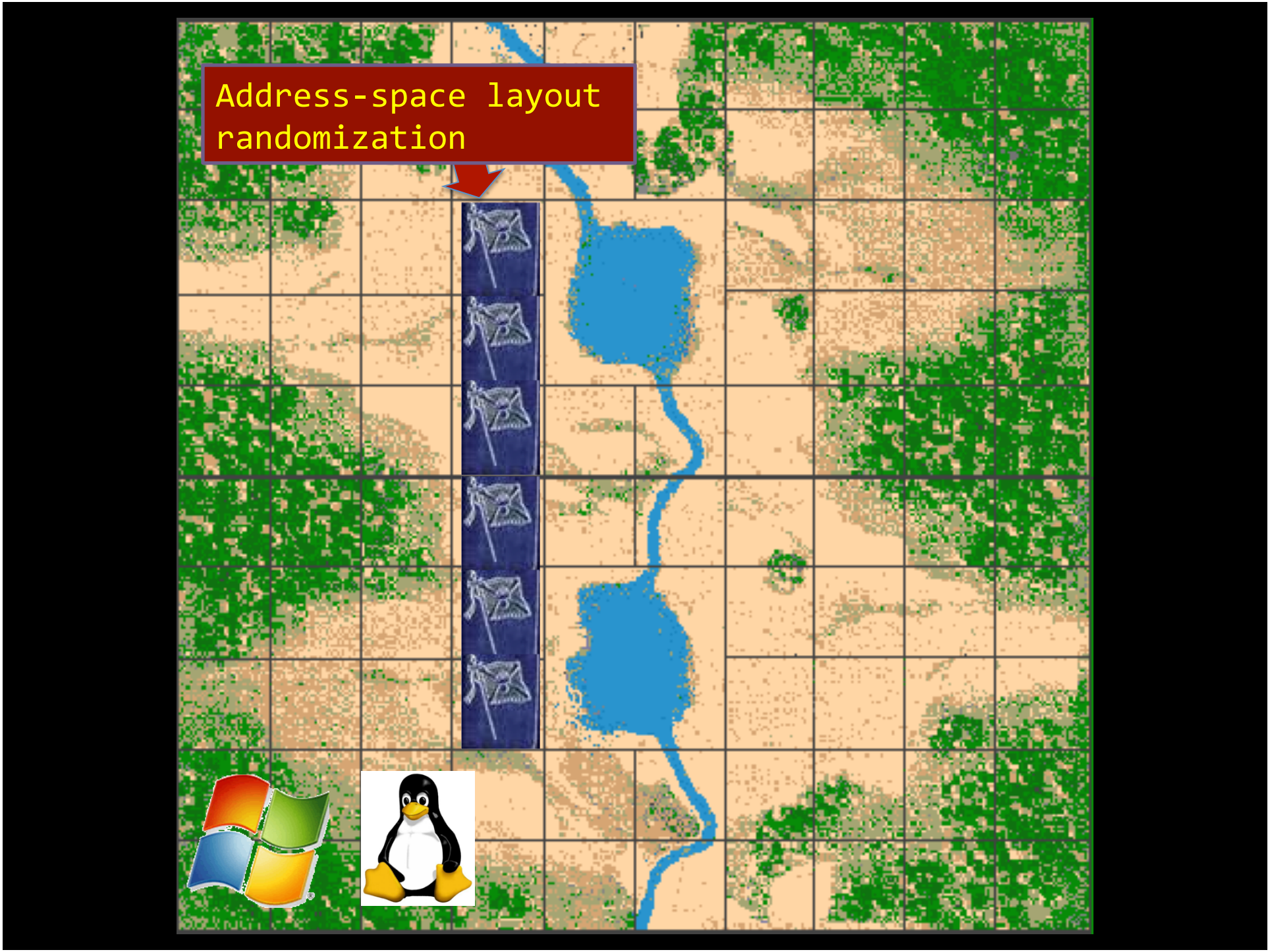

guard / unmapped page


Microsoft Office PowerPoint
Microsoft Office PowerPoint has encountered a problem and needs to close. We are sorry for the inconvenience.
The information you were working on might be lost. Microsoft Office PowerPoint can try to recover it for you.
Recover my work and restart Microsoft Office PowerPoint
Please tell Microsoft about this problem.
We have created an error report that you can send to help us improve Microsoft Office PowerPoint. We will treat this report as confidential and anonymous.
What data does this error report contain?
Why should I report to Microsoft?
Send Error Report
Don't Send

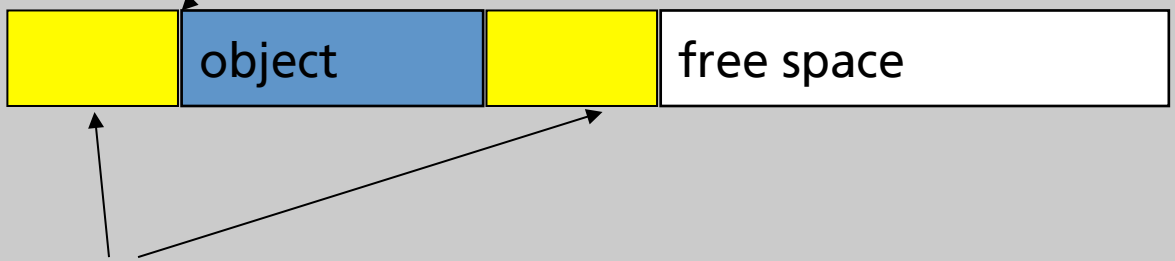






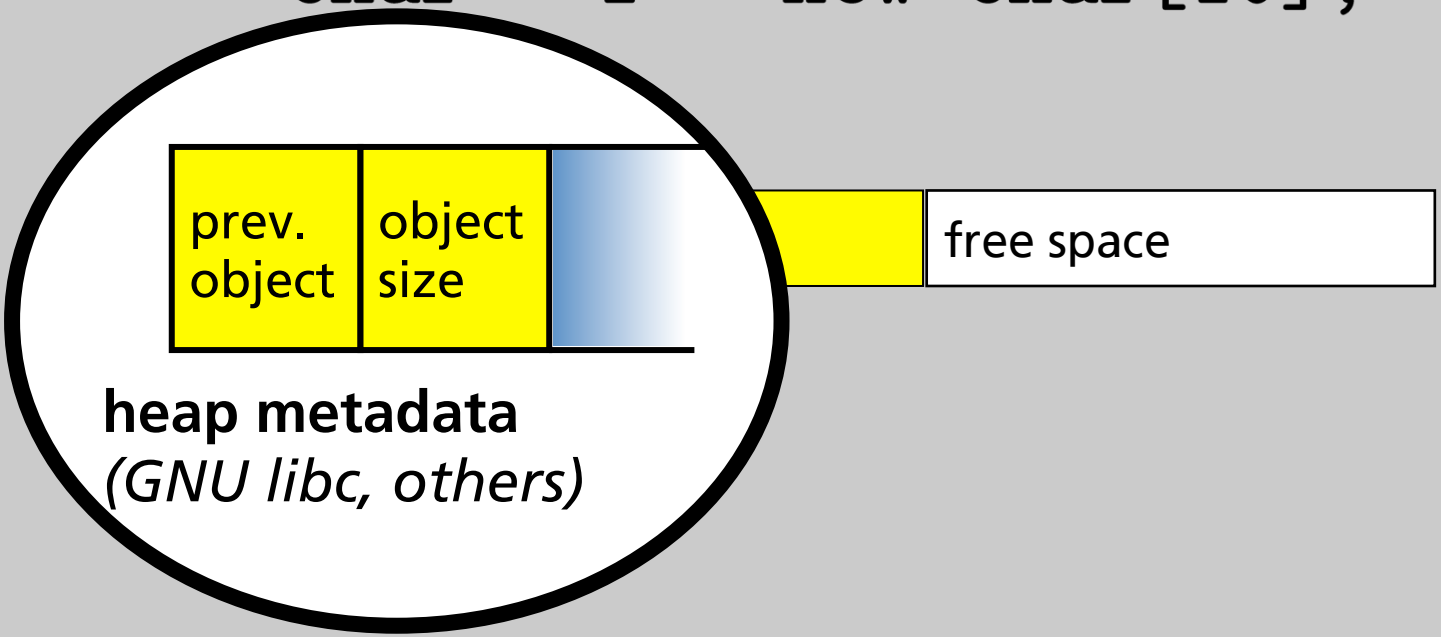

Address-space layout randomization

```
char * f = new char[10];
```

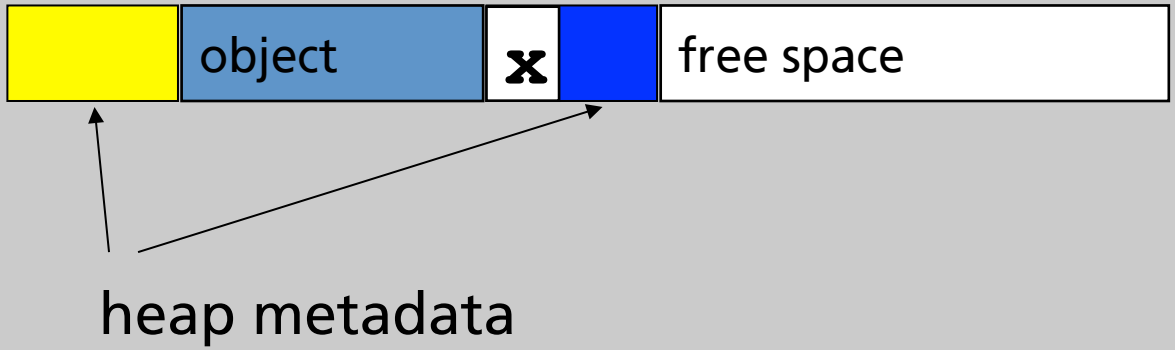


heap metadata

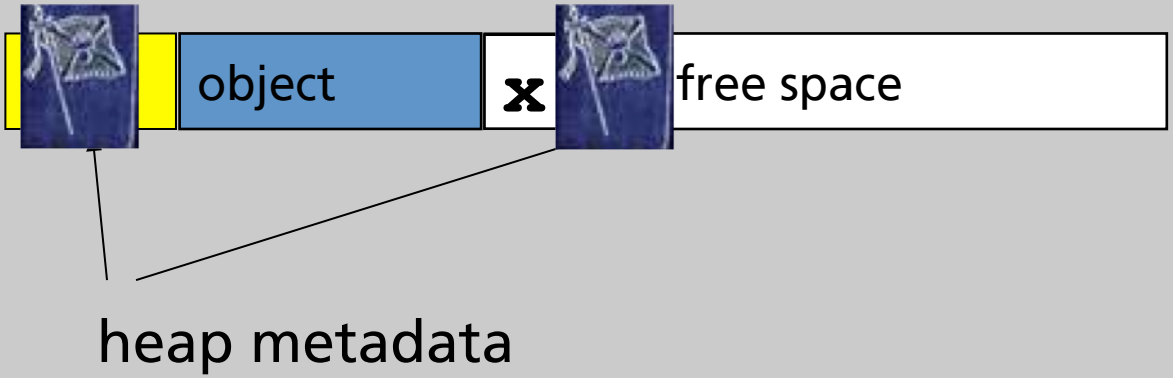
```
char * f = new char[10];
```

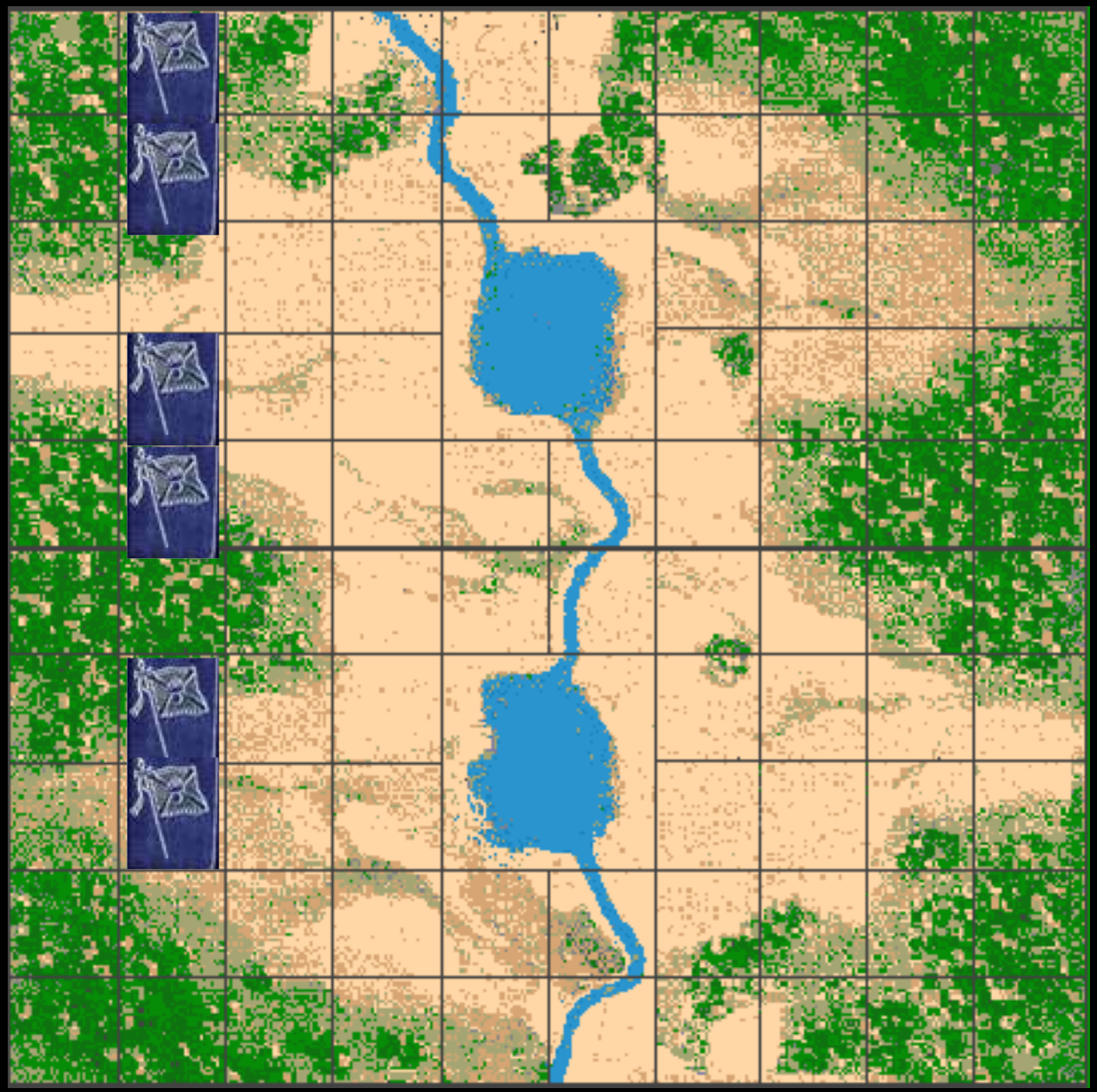


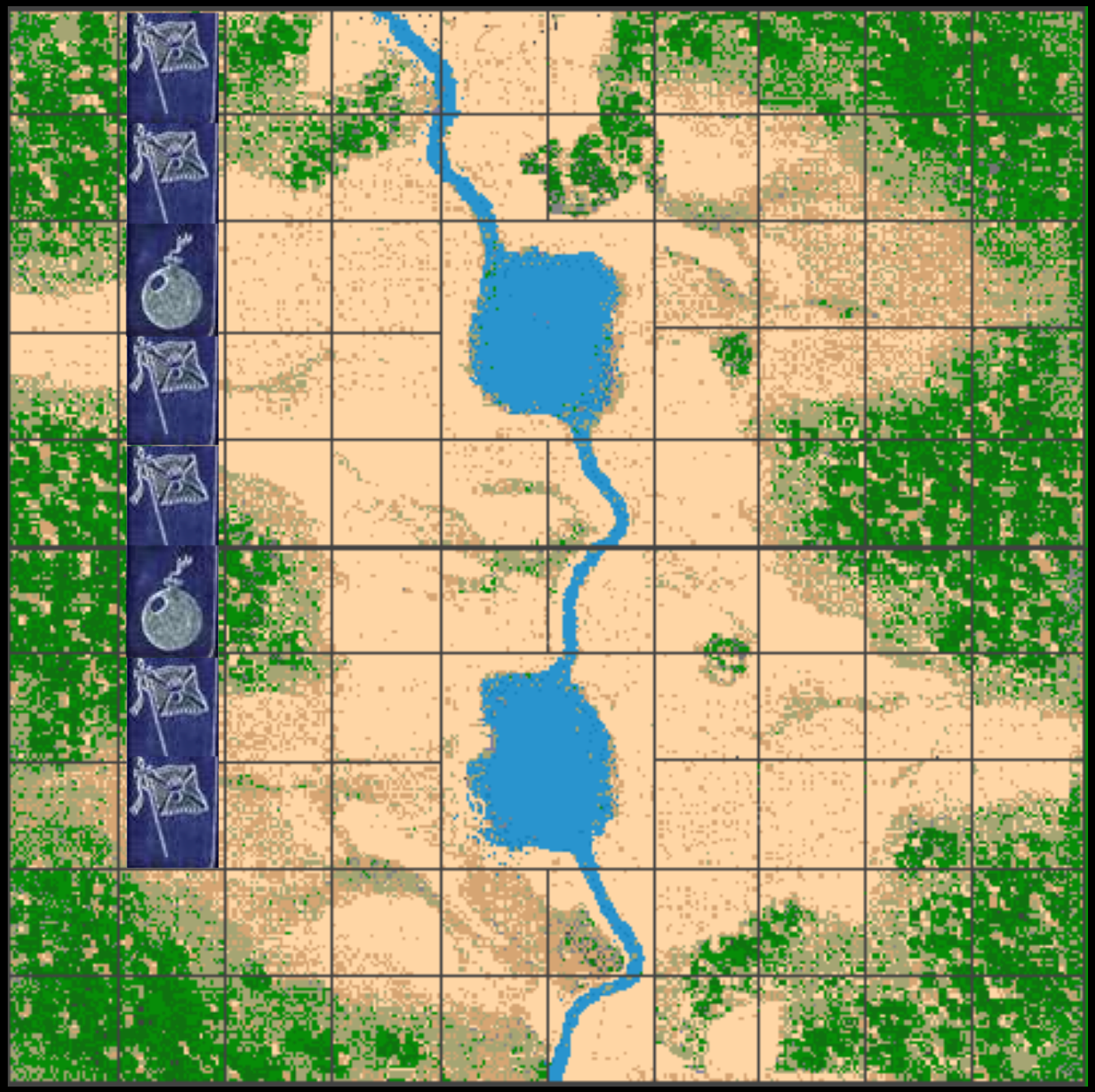
```
char * f = new char[10];
f[11] = 'x'; // adios heap
```

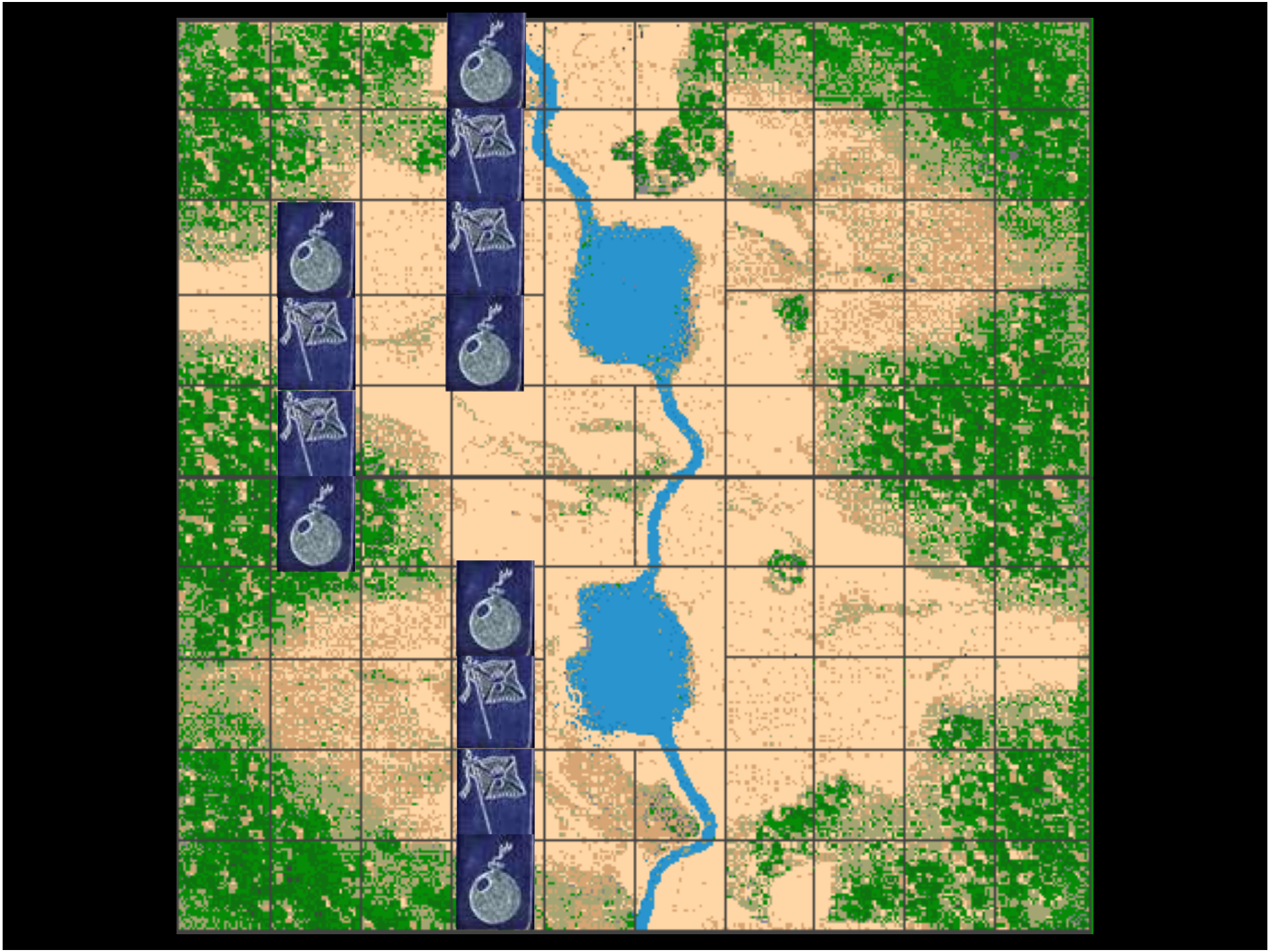


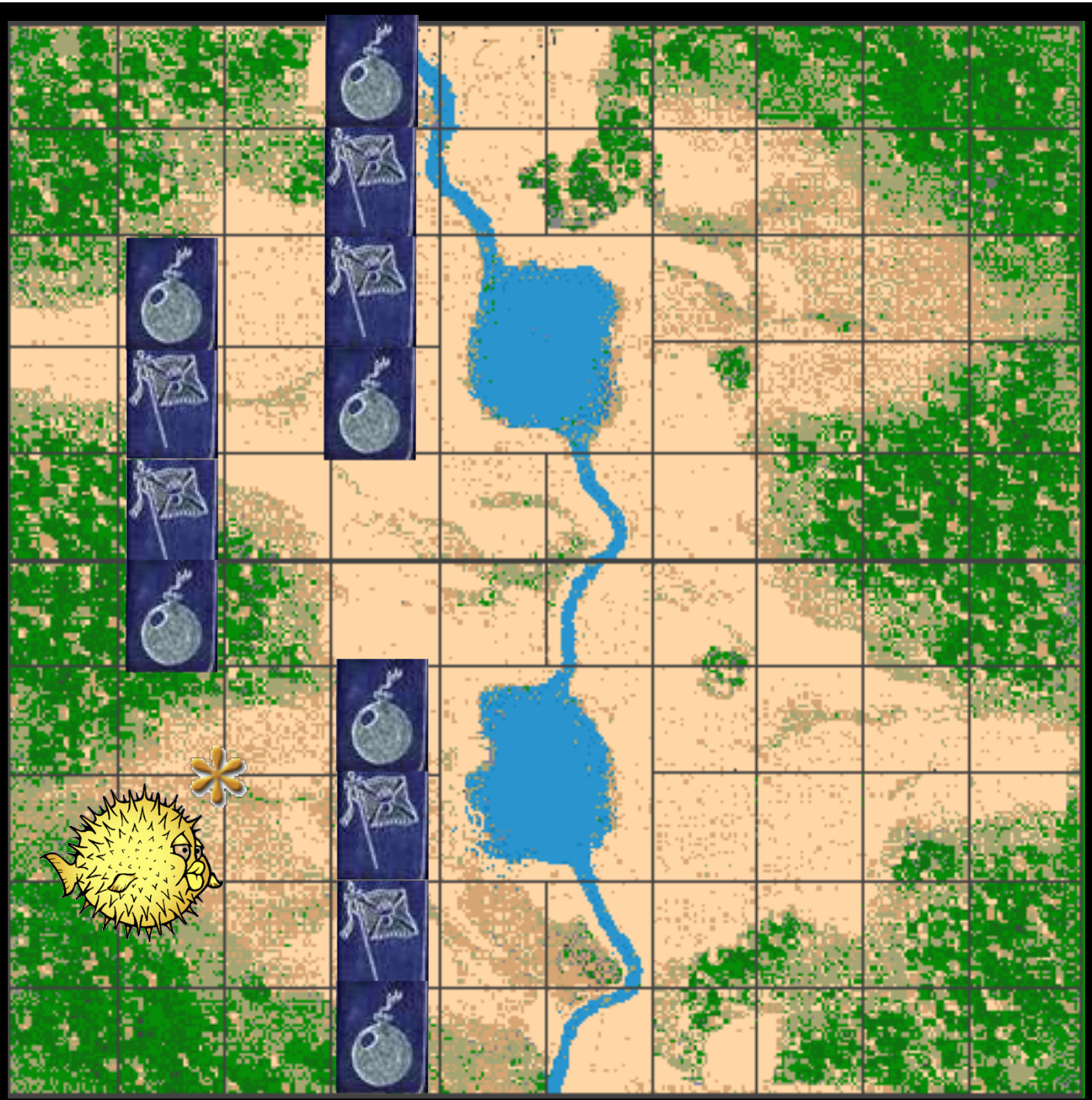
```
char * f = new char[10];
f[11] = 'x'; // adios heap
```

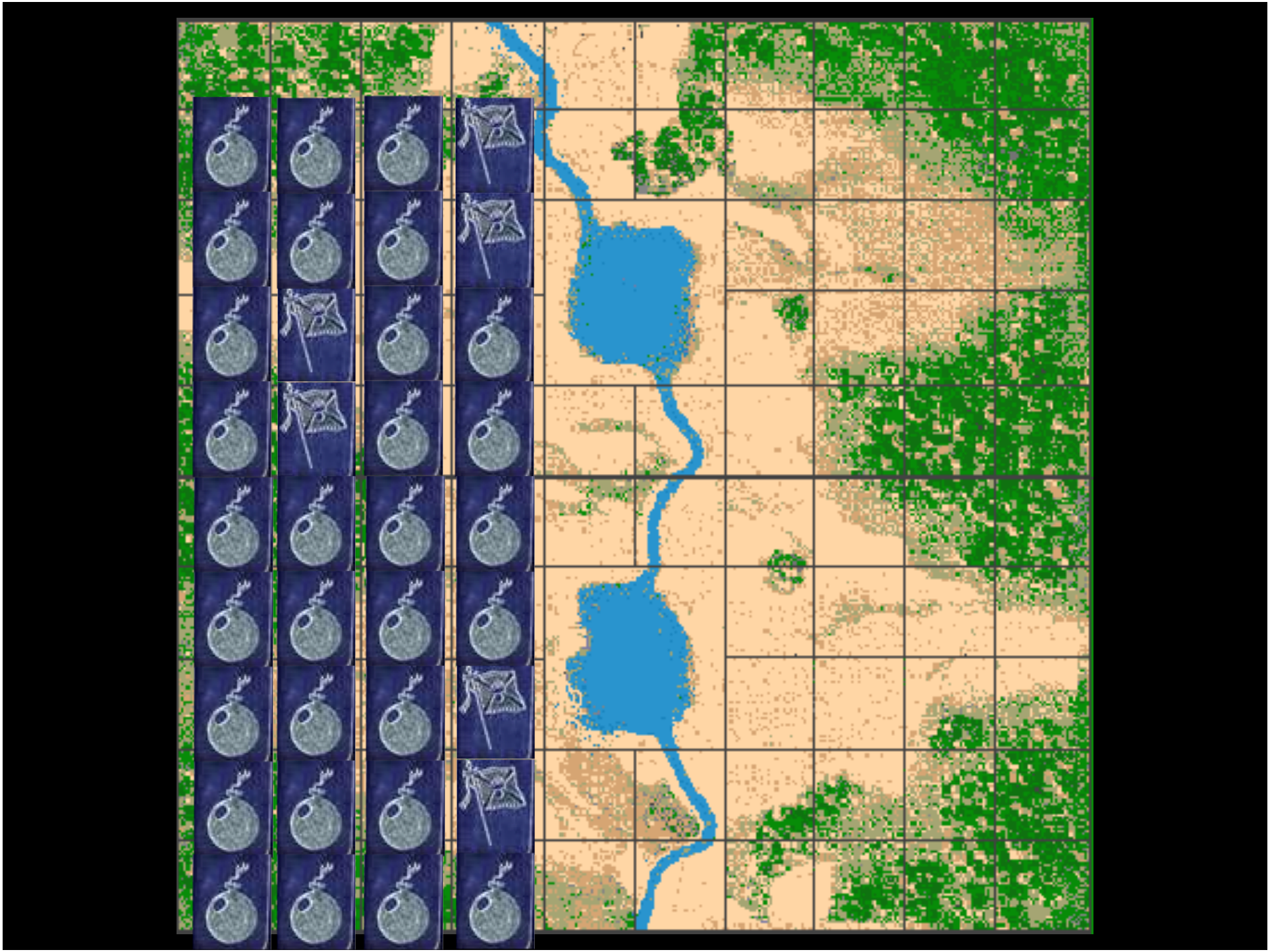


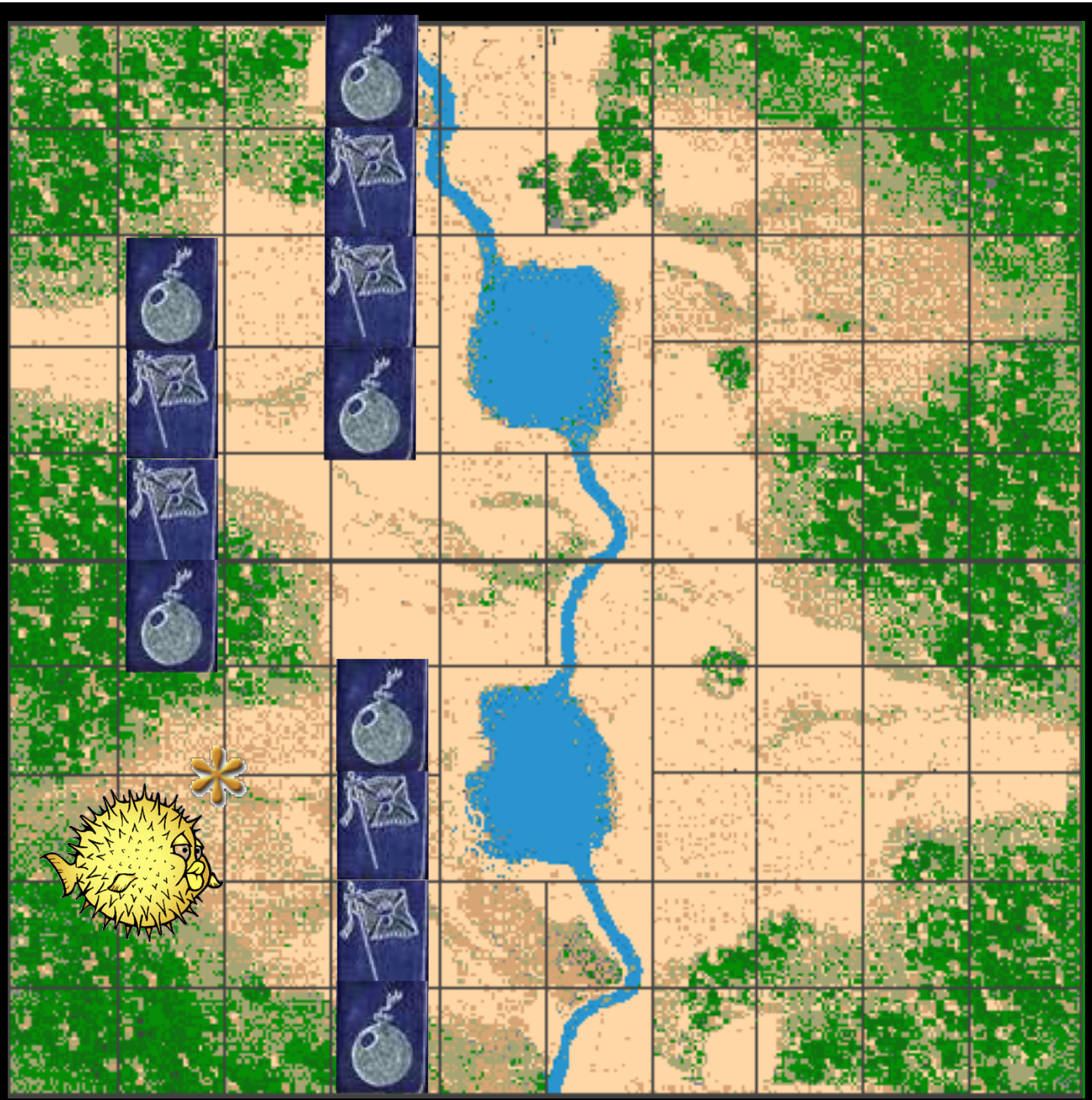


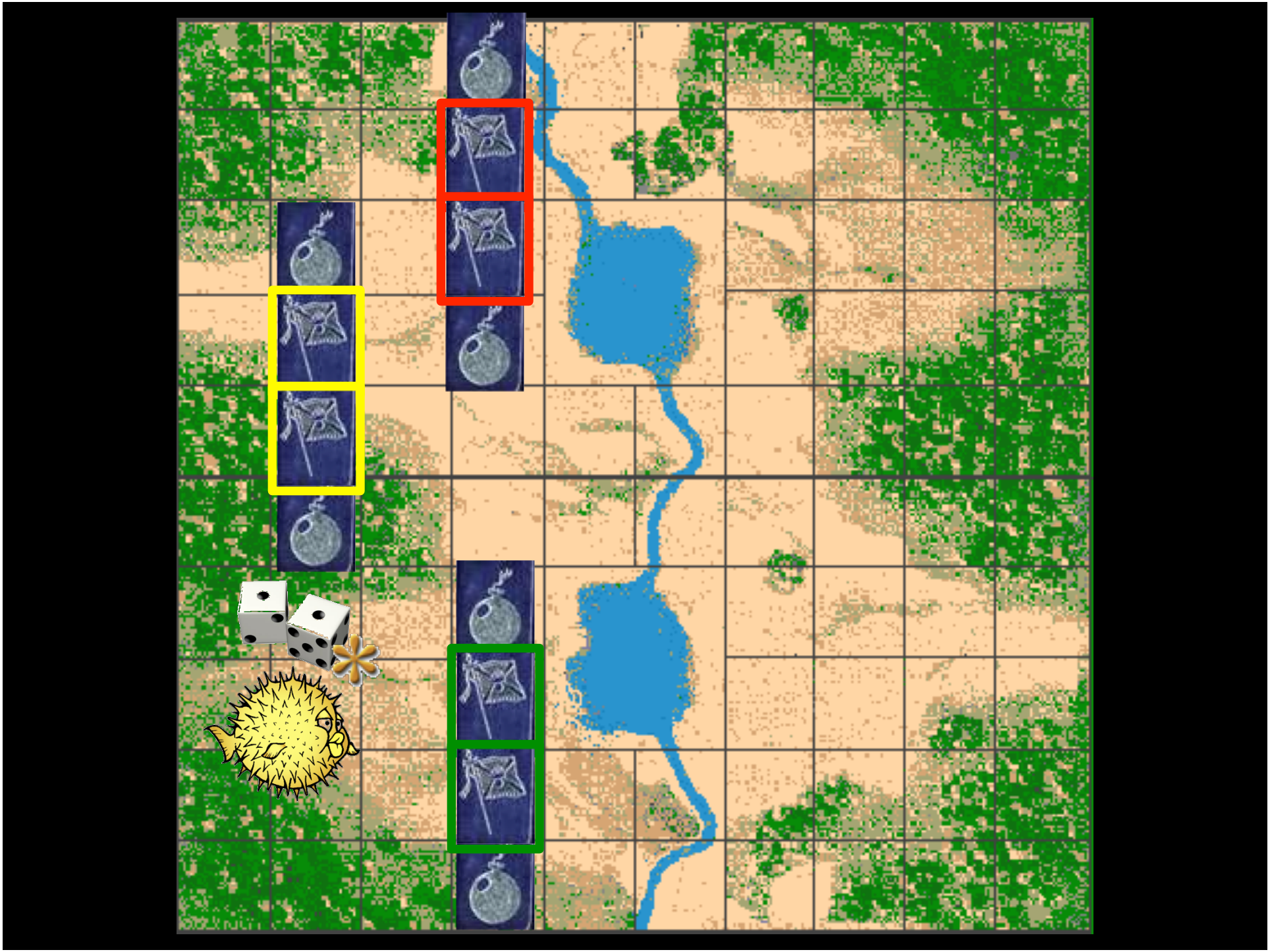


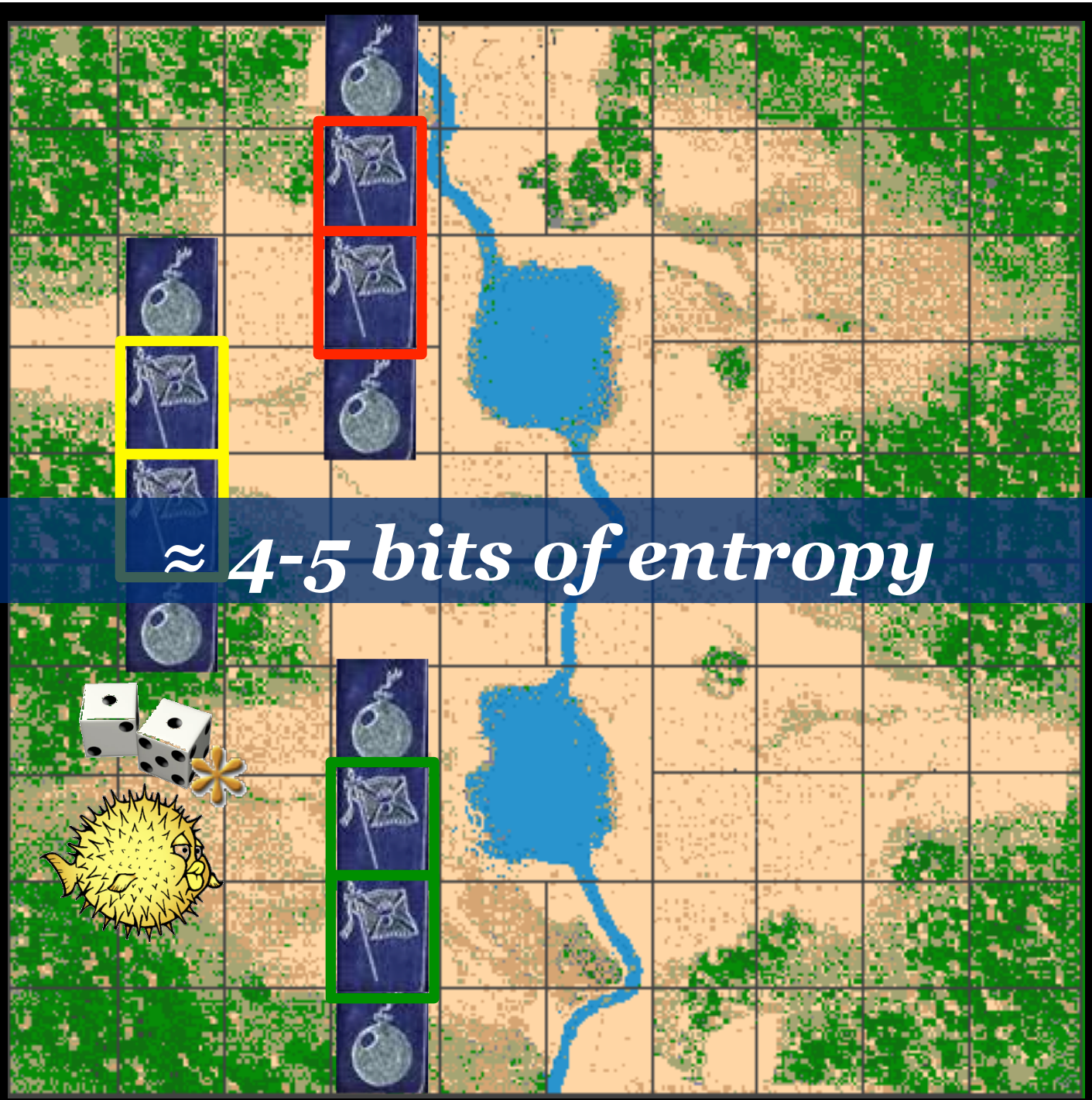


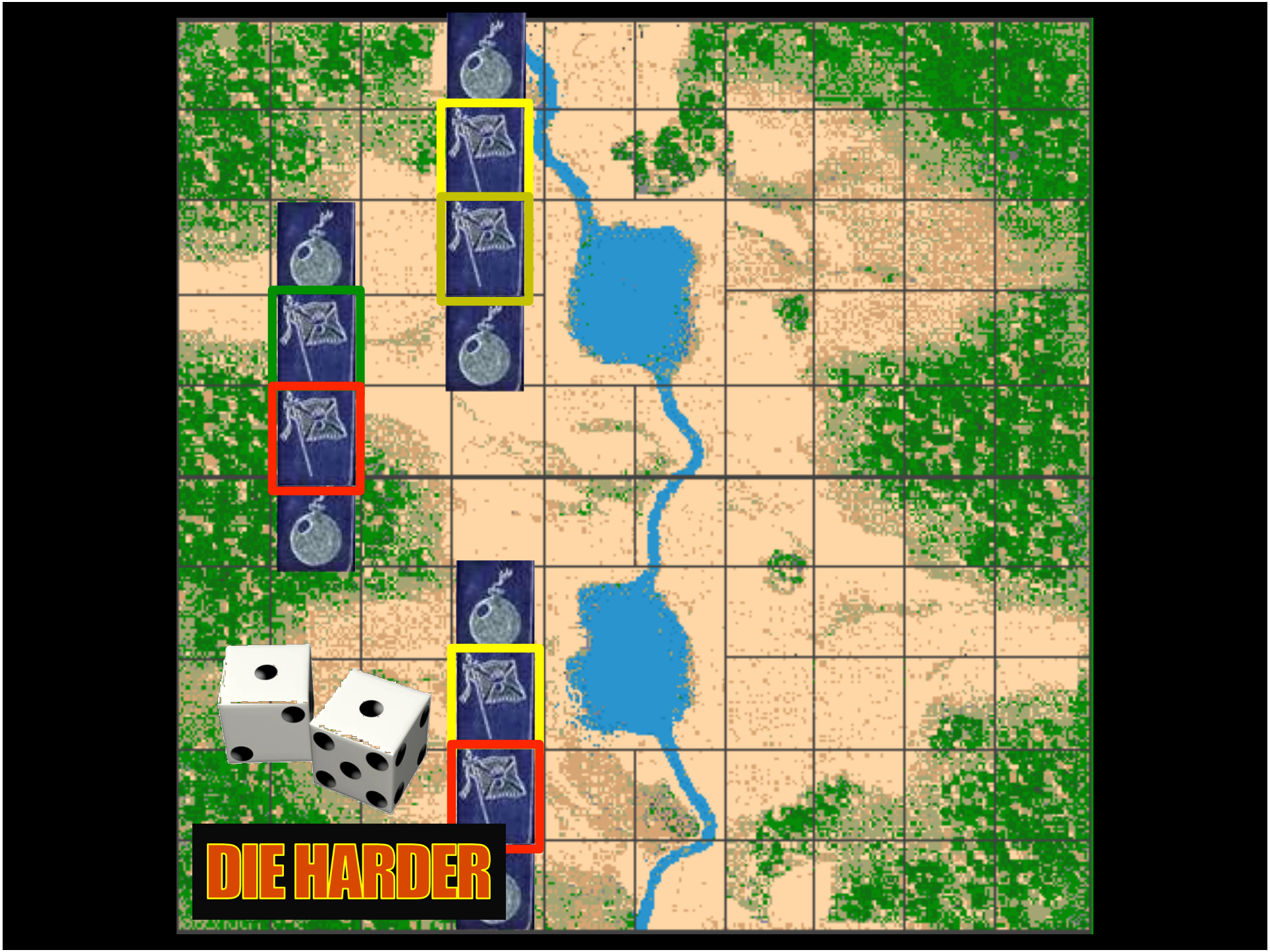


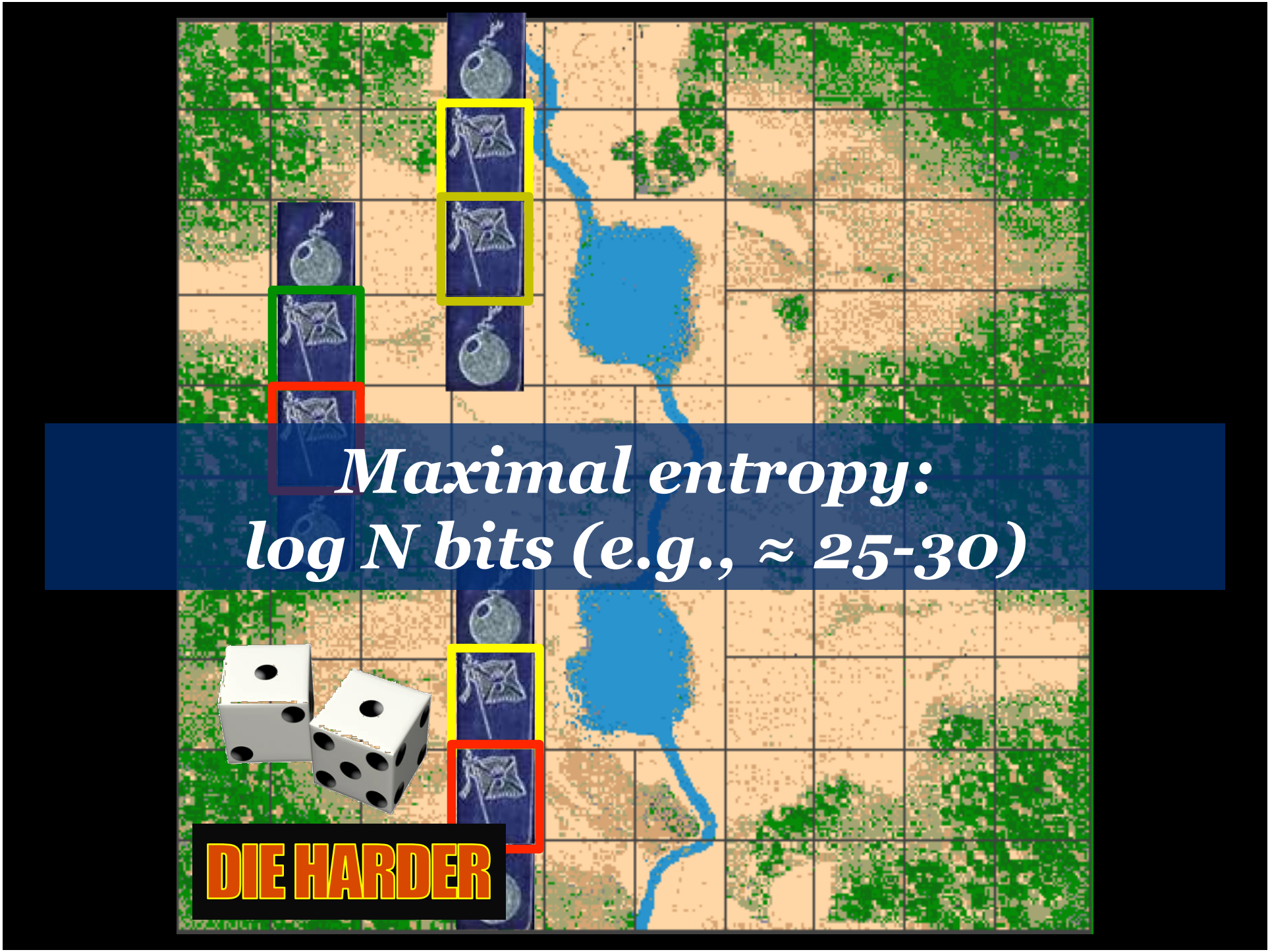


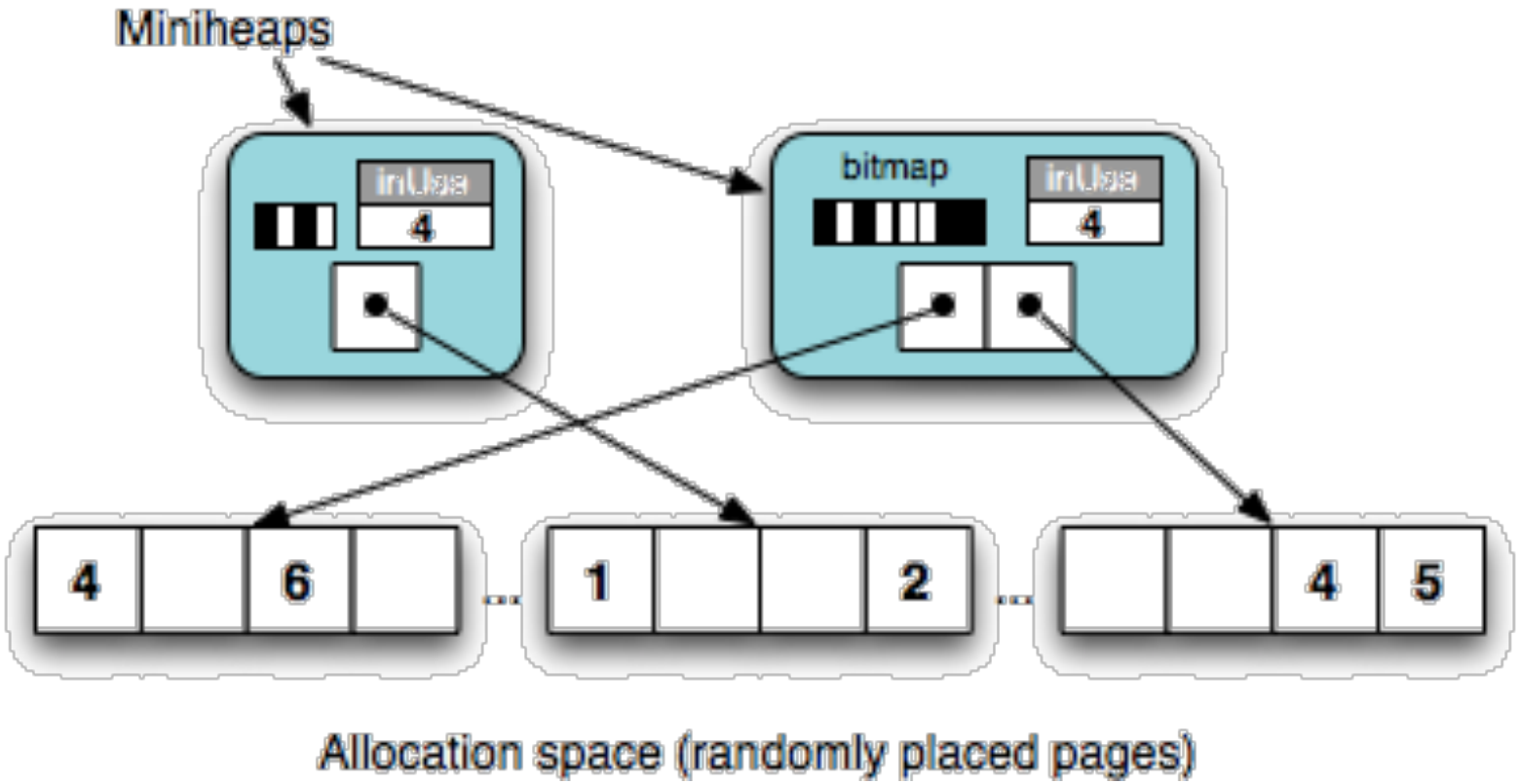


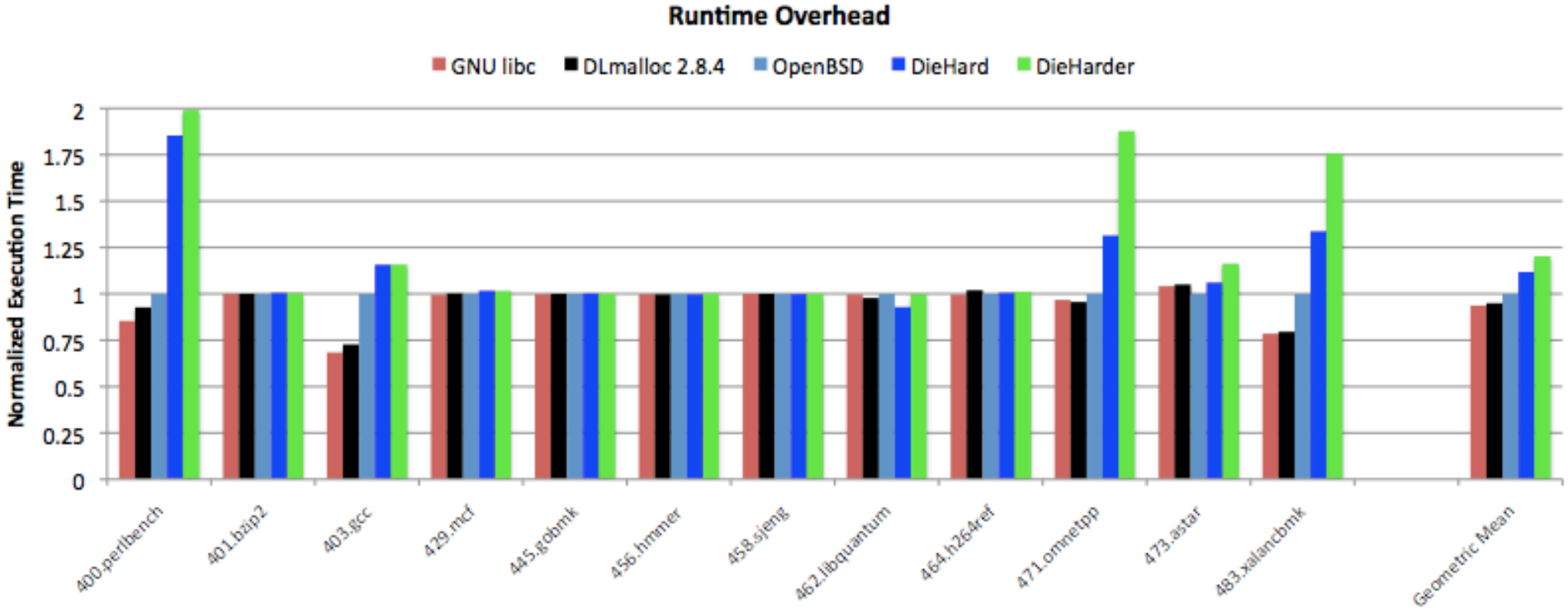



≈ 4-5 bits of entropy


DIE HARDER


Maximal entropy:
log N bits (e.g., ≈ 25-30)
DIE HARDER


Miniheaps
inUse
4
bitmap
inUse
4
4
6
1
2
4
5
Allocation space (randomly placed pages)


Runtime Overhead
GNU libc
DLmalloc 2.8.4
OpenBSD
DieHard
DieHarder
Normalized Execution Time
2
1.75
1.5
1.25
1
0.75
0.5
0.25
0
400.perlbench
401.bzip2
403.gcc
429.mcf
445.gobmk
456.hmmer
458.sjeng
462.libquantum
464.h264ref
471.omnetpp
473.astar
483.xalancbmk
Geometric Mean

DIE HARDER

44.2 sec

DIE HARDER

44.2 sec

41.6 sec

DIE HARDER

DieHarder: Securing the Heap

Gene Novark & **Emery Berger**

University of Massachusetts, Amherst