<The hacker's tool kit>

<x> Crowd sourcing

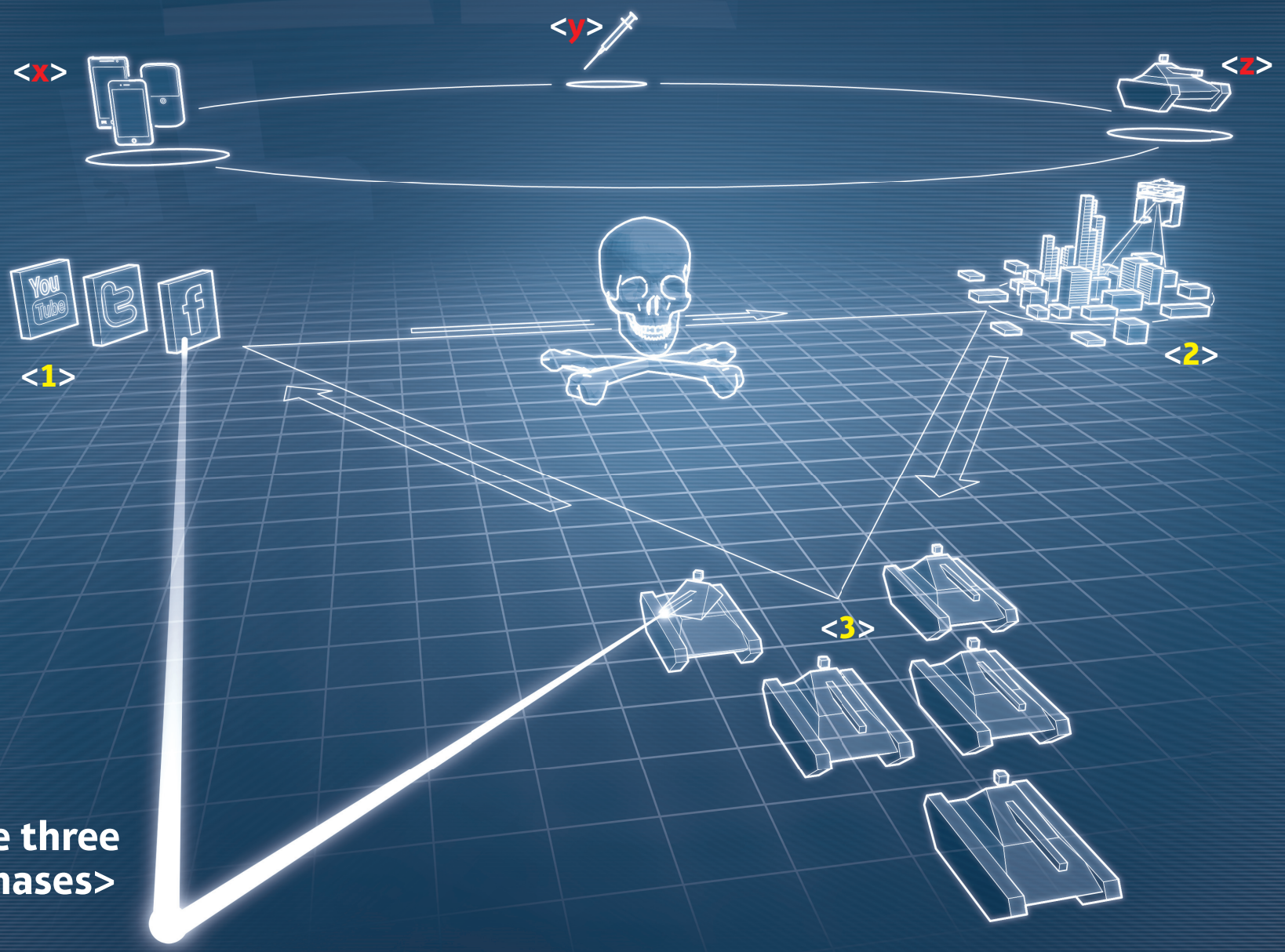
Anonymous's main innovation is its ability to recruit thousands of people to perform denial of service attacks. This relies on Anonymous making a compelling case for an attack. It also means that, if you're monitoring the right places, you may be given prior warning of an upcoming attack.

<y> SQL injections

Malicious code is inserted into a website and attacks from within. A popular tool for SQL injection is Havij, probably invented in Iran, which is designed to penetrate applications and steal data. It takes advantage of common vulnerabilities found in many websites.

<z> Low-orbit ion cannon

Designed by hackers using open source software as a tool for performing denial of service attacks. It probably consists of a few hundred lines of code and uses a web browser (on a PC, Mac or mobile) to flood a victim's website with excessive traffic (thereby shutting it down).



<There are three distinct phases>

<1> Recruitment and communication:

A small group of instigators use social media to elicit support and recruit for an attack. For example, YouTube videos are used to promote and rationalise the attack, while Facebook or Twitter followers are drafted in as volunteers to participate in the hacking campaign.

<2> Reconnaissance and application layer attack:

Once sufficient numbers have been recruited, the second phase begins. About 10-15 skilled hackers probe the website's vulnerabilities to identify weaknesses that could lead to a data breach.

<3> Distributed denial of service (DDoS) attack:

If phase 2 fails to expose the hidden data, Anonymous appeals to its 'non-technical' members (or lay people). Several hundred to a few thousand then download attack software (such as the Low Orbit Ion Cannon) and perform a DDoS attack.