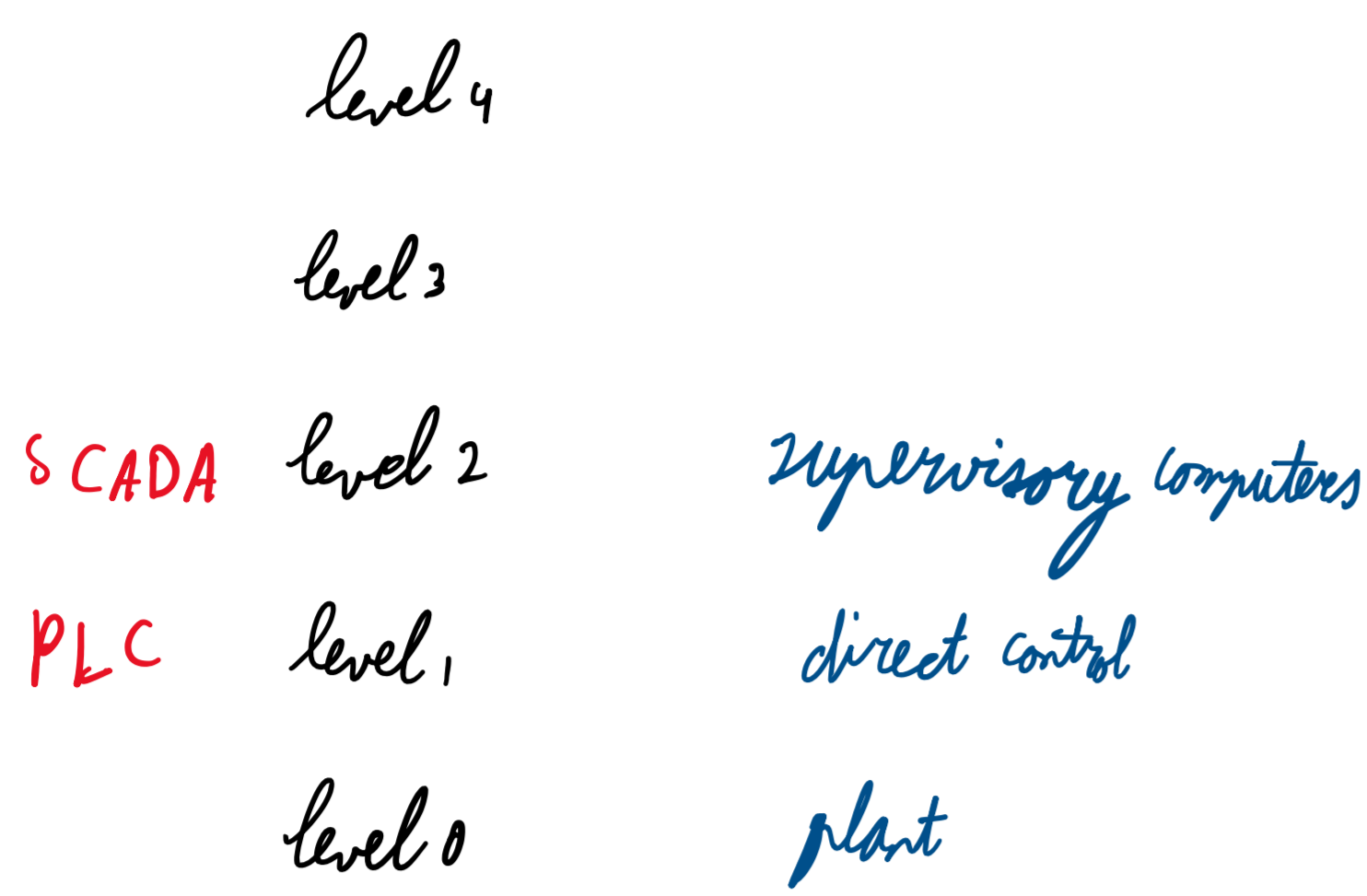


Targeted attacks on critical infrastructure

SCADA → supervisory control and data acquisition → sends control commands to PLC

PLC → programmable logic controller

Many communication protocols



SCADA systems were designed ^{20 years ago} in isolated situations, with no security in mind, for local access

today: connected throughout backoffice, allow remote control

lots of proprietary protocols, very hard to patch

very few attacks e.g. due to lack of monetary gain, lack of standardization in systems

supply chain attack: infect (USB of) maintenance supplier

Stuxnet phases

1. worm, with update
2. infects PLC, modifies programming
3. attack if in correct environment

Windows (4 zero-day vulnerabilities, rootkit, checks which AV is used, seeks target brand name) → modifies interface/API of OS to hide itself

finds PLC-related software, attacks via USB-stick, hooks into software DLL to replace code, includes rootkit

large frequency if ^{very specific} critical hardware was used

how:

spread through email, watering hole

gather information + gain persistent attacks

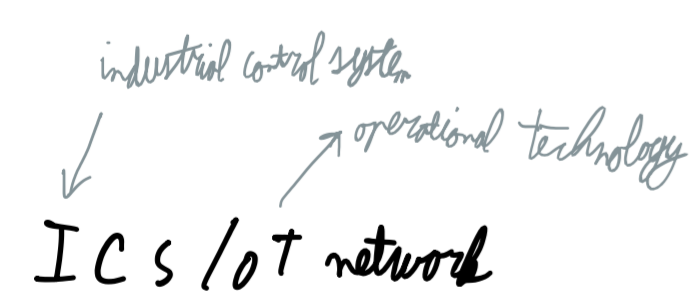
enumeration and qualification of network hosts

OPC servers + VPN connections to PLCs

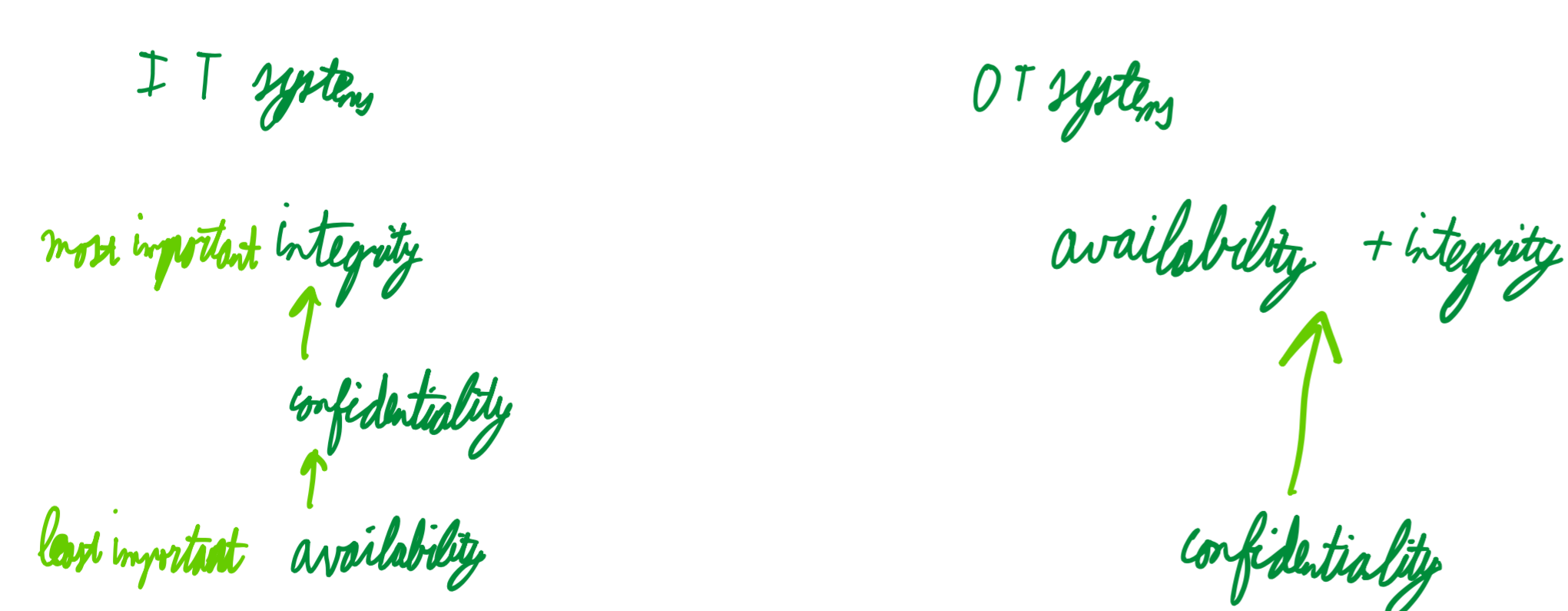
initially targeted aviation & defense
the US/EU

from compile time, can be derived as most likely Eastern European

Blockberg 3



- limited number of hosts
- same operations repeat over and over
- changes unless frequent



ICS is different from IT

- expensive to get inside
- difficult to recon attack on - is
- defender has no idea what happens inside

types of attackers:

- 0-days
- hacktivists
- nation states