CREATIVITY AND CYBER SECURITY

DR DEBI ASHENDEN,
CRANFIELD UNIVERSITY

Understanding of cyber security risk has traditionally been driven by the engineering and physical sciences where risk is seen as knowable and measurable. In the next issue of CREST Security Review we will focus on cyber security, highlighting new research that shows that these risks aren't best addressed through technological innovation.

'Specimens of IT Fauna' is one example of this human-centred approach and is the result of collaboration between social scientists, designers and technologists. The aim of this project was to use critical design to encourage cyber security practitioners and policy makers to re-conceptualise cyber security risk and think about technology in new and different ways.

These artefacts demonstrate the way critical design can be used to reflect on our understanding of cyber security and to envision future risks in a creative way.

SPECIMENS OF IT FAUNA

The internet is ubiquitous, yet its detailed inner workings remain wrapped in mystery. We rely on a wide range of myths, metaphors and mental-models to describe and communicate the network's abstract concepts and processes. Packets, viruses, worms, trojan horses, crawlers and cookies are all part of this imaginary bestiary of software.

This new mythology is one of technological wonders, such as live streams and cloud storage, but also of traps, monsters and malware agents. Folk tales of technology, however abstract and metaphorical, serve as our references and guidelines when it comes to making decisions and protecting ourselves from attacks or dangers.

Between educational props and memorabilia, this series of objects visualises and celebrates the abstract bestiary of the internet and acts as a tangible starting point to discuss our relationship to IT technology.

The artefacts were produced as part of the Visualisation and Other Methods of Expression (VOME) project, which was funded by the UK's Engineering and Physical Sciences Research Council (Grant number: EP/G002347/1) and led by Debi Ashenden at Cranfield University.

01
Web-crawler

Scale 6:1
The Web-crawler (also known as web-spider or web-robot) methodically patrols the network to index its contents.

(1) STP Wire Cat 6E
(2) Crawler
(3) Content ="follow"

02
Low Orbit Ion Cannon

Scale 1:100.000.000
The Low Orbit Ion Cannon, is a powerful weapon in the video game Command and Conquer. It is also the name of a piece of software used to carry out denial of service attacks.

(1) Botnet Zombies
(2) Botnet Handler
(3) Attack Leader
(4) LOIC
(5) DDoS Target

03
Blaster worm in SD card

Scale 5:1
Computer worms are standalone malware programs have the ability to replicate and spread their malicious 'payload' to other computers on a network.

(1) Replica
(2) Payload
(3) Data Damage