## Tekst 3

# The case for the cyberdefence

*Governments and companies must co-operate more closely*

1 The march of cyberwar from science fiction to fact continues apace. On Wednesday, Google revealed that, for the second time in two years, it had fallen victim to a cyberattack launched in China. The latest assault targeted users of its Gmail service ─ including senior US officials ─ who were sent customised bogus e-mails that tricked them into giving away the passwords to their e-mail accounts.

2 "Spear-phishing", as this practice is known, is already common: British government departments are the target of 1,000 attacks per month. As the world's reliance on computer networks grows, such threats will only become more acute. It is crucial, therefore, that governments and companies take steps now to combat this problem.

3 Despite moves this week by the US government to classify cyberattacks as an act of war (which might allow military retaliation), cold-war-style deterrence is not a realistic option. As the uncertainty over the identity of Google's attackers shows, cyberweapons can be used with a degree of anonymity. Threats of reprisals (and international treaties) are therefore no more than empty words.

4 That puts a premium on defence. Here there is much that governments and companies can do, both individually and in concert. Companies should isolate sensitive systems from both the internet and other internal networks. They must also control gadgets used by staff more tightly (Stuxnet, after all, spread through flash-drives). Such steps will be easier to co-ordinate if the role of the chief technology officer is boosted.

5 Other changes will require a radical shift in corporate culture. One of the difficulties in fighting cybercrime is that companies rarely share information on security breaches. That allows attackers to perform the same trick on many targets. To combat this, companies must get used to pooling details of security breaches with their rivals. Anonymising the information might make this process easier.

6 For their part, governments must include the private sector in their defensive planning. An attack on the banking sector, for example, could be crippling. Yet most cyberdefence agencies focus on protecting government and the military. That must change. Governments should also enforce higher security standards for software products.

7 Ultimately, however, systems are no securer than the staff who run them. The latest attack on Google exploited not technical but human frailty. That is something no amount of technology can cover.

*Financial Times, 2011*

## Tekst 3 The case for the cyberdefence

1p **4** What is the function of paragraphs 1 and 2?

- **A** to emphasise that cyberattacks need to be addressed urgently
- **B** to illustrate that education about cyberdefence is of utmost importance
- **C** to introduce the problems authorities encounter when prosecuting cybercriminals
- **D** to point out the cybertactics deployed by enemies of national governments

"That puts a premium on defence." (paragraph 4)

1p **5** What is the underlying reason?

- **A** Considerable difficulty is experienced in identifying the enemy to be targeted.
- **B** Internal political dissension makes governments reluctant to carry out their threats.
- **C** The military response required would entail disproportionate collateral damage.

1p **6** How does paragraph 7 relate to the rest of the article?

- **A** It concludes the main line of argument.
- **B** It downplays the main line of argument.
- **C** It ridicules the main line of argument.
- **D** It summarises the main line of argument.

**Bronvermelding**

*Een opsomming van de in dit examen gebruikte bronnen, zoals teksten en afbeeldingen, is te vinden in het bij dit examen behorende correctievoorschrift, dat na afloop van het examen wordt gepubliceerd.*