Positive and negative liberty

Oxford philosopher and historian Isaiah Berlin distinguishes:

- **positive** liberty, or freedom to realize your goals
  ("I'm my own master")
- **negative** liberty, or freedom from interference by others
  ("I'm a slave to no man")

In the context of the internet

- in the early days internet is mostly associated with **positive**
  liberty, as a platform for free exchange of ideas, creating
  transparency & democracy, against monopolists/authorities etc
  - now "cyber utopianism", eg in **freedom online** movement
- Increasingly, internet affects **negative** liberty: there is much
  out there that you don’t wish to be confronted with.

Three books by insiders

1. Richard Clarke, *Cyber War*, 2010
   [By former US national coordinator for counterterrorism, and later
   for security, infrastructure protection.]
2. David Oman, *Securing the State*, 2010
   [By former GCHQ director (UK)]
   [By current White House “cyber security czar.”]

They give interesting overviews & anecdotes, but remain
rather superficial; however, they may serve as “eye-openers”.

The real extent of the problems remain hard to assess, and
insiders have their own bias/interests
Cybercrime: common distinction

- old crimes, new methods
  - fraud, extortion, identity theft
  - stalking, grooming, child pornography, . . .
  - copyright violation
- Some of these have undergone huge quantitative changes

new crimes, targeting computers/networks
- spreading malware, running botnets
- (DOS) attacks, defacing websites, . . .
- violations of network security

Cyber-security / historical developments

- Hackers/phreakers exploring/exploiting new, unprotected infrastructure, out of curiosity or to gain (cheap) access
  - before computer crimes laws existed (< 1990)
  - in NL see Hack-Tic magazine for “techno-anarchists” (archive at hacktic.nl)
- Individuals exploiting/damaging poorly protected infrastructure
  - famous viruses (Melissa, Nimba, Code Red, I love you, . . .)
  - introduction of laws and international coordination (eg. via cybercrime units & CERT’s)
  - first toolboxes for script kiddies
- Organized crime & stately actors, against moderately protected infrastructure
  - underground economy in stolen goods / tools / vulnerabilities
  - start of critical infrastructure protection

Some difficult questions (after Richard Clarke)

- Mix of cyber and kinetic warfare:
  - Iraqi military officers received US warning/advise email on their military accounts before the 2003 gulf war started
  - Estonia (2007), several weeks under DOS attack after moving a sensitive Russian statue: wake-up call for NATO
  - Georgia (2008) DOS attack preceded Russian invasion
  - DOS attack on US and South-Korean computers at the time of several North-Korean (test) missile launches
- Many countries now have cyberwar capabilities.
  - frequently mentioned: US, China, Russia, Iran, North Korea, Israel, . . .
  - modern societies are most vulnerable to attacks

High profile cyber incidents

- GhostNet botnet (2009), with many “high-value” infections
  - primarily free-Tibet activists, but also embassies
  - several control servers located in China
- Stuxnet (2010), aimed at Iranian nuclear installations
  - unprecedented complexity, infecting both Windows & Scada
  - possibly part of US & Israeli cyber war against Iran (also: Duqu, . . .)
- DigiNotar (2011)
  - Fake certificates, especially for gma11.com, used in Iran
  - Hacker could have placed all 50K valid certificates on blacklist

Question: why should public authorities clean up the mess when private parties are reluctant to employ proper security technology?

(Also applies to OV-chipkaart, where they seem to be wiser now)

Skimming of NL cards in NL should decrease by 1/1/12, through use of EMV-chip — for which attacks are emerging now.
- vulnerabilities still exist abroad

What is happening?

- Mix of cyber and kinetic warfare:
  - Iraqi military officers received US warning/advise email on their military accounts before the 2003 gulf war started
  - Estonia (2007), several weeks under DOS attack after moving a sensitive Russian statue: wake-up call for NATO
  - Georgia (2008) DOS attack preceded Russian invasion
  - DOS attack on US and South-Korean computers at the time of several North-Korean (test) missile launches

- Many countries now have cyberwar capabilities.
  - frequently mentioned: US, China, Russia, Iran, North Korea, Israel, . . .
  - modern societies are most vulnerable to attacks

Financial cybercrime example: skimming

- Serious criminal business in NL, with yearly 30M+ stolen from customer accounts (apparently mostly by Romanians)
- The technical vulnerabilities are known since 20 years
- Banks slowly improve technology; cheaper to repay damages
- NL police launches “national skimming point”, late 2011

- Should these be seen as “acts of war”?

- Question: why should public authorities clean up the mess when private parties are reluctant to employ proper security technology?

(Also applies to OV-chipkaart, where they seem to be wiser now)

Skimming of NL cards in NL should decrease by 1/1/12, through use of EMV-chip — for which attacks are emerging now.
- vulnerabilities still exist abroad

- Mix of cyber and kinetic warfare:
  - Iraqi military officers received US warning/advise email on their military accounts before the 2003 gulf war started
  - Estonia (2007), several weeks under DOS attack after moving a sensitive Russian statue: wake-up call for NATO
  - Georgia (2008) DOS attack preceded Russian invasion
  - DOS attack on US and South-Korean computers at the time of several North-Korean (test) missile launches

- Many countries now have cyberwar capabilities.
  - frequently mentioned: US, China, Russia, Iran, North Korea, Israel, . . .
  - modern societies are most vulnerable to attacks

- Question: why should public authorities clean up the mess when private parties are reluctant to employ proper security technology?

(Also applies to OV-chipkaart, where they seem to be wiser now)

Skimming of NL cards in NL should decrease by 1/1/12, through use of EMV-chip — for which attacks are emerging now.
- vulnerabilities still exist abroad

- Mix of cyber and kinetic warfare:
  - Iraqi military officers received US warning/advise email on their military accounts before the 2003 gulf war started
  - Estonia (2007), several weeks under DOS attack after moving a sensitive Russian statue: wake-up call for NATO
  - Georgia (2008) DOS attack preceded Russian invasion
  - DOS attack on US and South-Korean computers at the time of several North-Korean (test) missile launches

- Many countries now have cyberwar capabilities.
  - frequently mentioned: US, China, Russia, Iran, North Korea, Israel, . . .
  - modern societies are most vulnerable to attacks

- Question: why should public authorities clean up the mess when private parties are reluctant to employ proper security technology?

(Also applies to OV-chipkaart, where they seem to be wiser now)

Skimming of NL cards in NL should decrease by 1/1/12, through use of EMV-chip — for which attacks are emerging now.
- vulnerabilities still exist abroad

- Mix of cyber and kinetic warfare:
  - Iraqi military officers received US warning/advise email on their military accounts before the 2003 gulf war started
  - Estonia (2007), several weeks under DOS attack after moving a sensitive Russian statue: wake-up call for NATO
  - Georgia (2008) DOS attack preceded Russian invasion
  - DOS attack on US and South-Korean computers at the time of several North-Korean (test) missile launches

- Many countries now have cyberwar capabilities.
  - frequently mentioned: US, China, Russia, Iran, North Korea, Israel, . . .
  - modern societies are most vulnerable to attacks

- Question: why should public authorities clean up the mess when private parties are reluctant to employ proper security technology?

(Also applies to OV-chipkaart, where they seem to be wiser now)

Skimming of NL cards in NL should decrease by 1/1/12, through use of EMV-chip — for which attacks are emerging now.
- vulnerabilities still exist abroad

- Mix of cyber and kinetic warfare:
  - Iraqi military officers received US warning/advise email on their military accounts before the 2003 gulf war started
  - Estonia (2007), several weeks under DOS attack after moving a sensitive Russian statue: wake-up call for NATO
  - Georgia (2008) DOS attack preceded Russian invasion
  - DOS attack on US and South-Korean computers at the time of several North-Korean (test) missile launches

- Many countries now have cyberwar capabilities.
  - frequently mentioned: US, China, Russia, Iran, North Korea, Israel, . . .
  - modern societies are most vulnerable to attacks

- Question: why should public authorities clean up the mess when private parties are reluctant to employ proper security technology?

(Also applies to OV-chipkaart, where they seem to be wiser now)
Cybersecurity is the freedom of being free of danger or harm caused by cyber weapons or other weapons. It is described as a negative freedom, not as a scientific discipline or area of activities.

More such questions

- If we are attacked with cyber weapons, under what circumstances would, or should, we respond with kinetic weapons? How much of the answer to this question should be publicly known in advance?
- Should the line between peace and cyber war be brightly delineated, or is there an advantage to us in blurring that distinction?
- What level of command authority should authorize the use of cyber weapons, select the weapons, and approve the targets?
- Are there types of targets that we believe should not be attacked using cyber weapons? Do we attack them anyway if similar U.S. facilities are hit first by cyber or other weapons?
- Despite huge budget cuts, NL has decided to allocate 50M€ for taskforce cyber, headed by col. Hans Folmer.
- Primarily invested in strengthening defensive capabilities (detection, monitoring, hardening).
- Funding goes in part to DefCERT, MIVD.
- Until 2015 no offensive capabilities.
- Legal issues must be clarified first.
- Latest plans: use cyber reservists for calamities and/or military operations.
- Maybe not a bad idea.

In 2011 an overview of cyber security threats has been written (by GovCert, with input from police & intelligence communities).


Systematic approach puts threats in context:
- Assets: what should be protected
- Threats, related to these assets, together with risk, eg. as chance × impact
- Controls, to counter these threats

Cybersecurity is the freedom of being free of danger or harm caused by cyber weapons or other weapons. It is described as a negative freedom, not as a scientific discipline or area of activities.

### Cybersecurity Definition in NL Cyber Security Strategy

Cybersecurity is the freedom of being free of danger or harm caused by cyber weapons or other weapons. It is described as a negative freedom, not as a scientific discipline or area of activities.

- Not clear! In Wikipedia it is synonym to computer security.
- Interpretation used here: combination of:
  - Cybercrime “in the large”, threatening infrastructure
  - Cyber defense/warfare

### NL Cyber Security Strategy

Cybersecurity is the freedom of being free of danger or harm caused by cyber weapons or other weapons. It is described as a negative freedom, not as a scientific discipline or area of activities.

- Cybersecurity is the freedom of being free of danger or harm caused by cyber weapons or other weapons. It is described as a negative freedom, not as a scientific discipline or area of activities.

### Threat Overview (from Cyber Security Beeld)

<table>
<thead>
<tr>
<th>Deelobject</th>
<th>Overheid</th>
<th>Overheid</th>
<th>Burgers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nationale</td>
<td>Digitale storing en ophoping</td>
<td>Digitale storing en ophoping</td>
<td></td>
</tr>
<tr>
<td>Penrose-organisaties</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Houtskool</td>
<td>Digitale storing en ophoping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verenigde</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nederland</td>
<td>Digitale storing en ophoping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scholen</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bedrijven</td>
<td>Digitale storing en ophoping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staat</td>
<td>Digitale storing en ophoping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitale</td>
<td>Digitale storing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Threat Scenario I

- Assume the NL cabinet receives the following message:
  *If you do not cut all ties with Taiwan within one month, your flood protection gates will be opened electronically!*
- Is this something one can ignore?
  *If not, what to do about it?*
- Summoning the Chinese ambassador is probably not helpful: "China is a peaceful nation; we don’t use such methods; these are probably maverick hackers."
- Making sure such attacks are not possible is probably best.
  *But then the infrastructure must already be hardened now.*
- What is “cyber” about this? Such threat messages can also contain physical/kinetic threats. What is the difference?
Critical infrastructure protection

- Critical infrastructure means: gas, water, electricity, fuel, telecom, dikes, etc.
- Much of this has been digitized, in two phases:
  1. local devices (sensors, actuators) running on simple dedicated processors (so-called scada systems)
  2. networked systems, mostly composed of COTS hard/software
- Big problem: these scada systems have no protection built in
  1. they were never designed to run in hostile environments
  2. or to withstand a stuxnet level of aggression/sophistication
- What is the advantage of a digital attack on this infrastructure?
  1. compared to blowing up a few electricity poles

Threat scenario II

- US asks for extradition of Rop Gonggrijp, on the basis of his WikiLeaks participation (in the release of the “Collateral Murder” video in April 2010)
- NL trusts US legal system, so hands him over to US authorities (NL offers little or no protection to its citizens)
- Then, the shit hits the fan:
  1. Anonymous, LulzSec, CCC and everyone else in the world attacks NL government infrastructure
  2. many people in ISPs, CERTs etc sympathise with Gonggrijp, look the other way, and don’t stop the flood
  3. sites are unreachable for weeks, government secrets are published
- How realistic is this one? What to do about it?

Advantages of cyber conflicts

1. Little physical risk involved for the attacker
2. Attacker can stay below the radar, for a long time
3. When the attack is eventually detected, attribution is hard
4. It provides plausible deniability for stately actors to conduct “war-light”, eg. via blackmail, disruption (like against Iran)
5. It increases the power of hacktivists / guerilla-like groups / ..., in a-symmetric conflicts

Internet freedom for who?

- for dissidents in faraway countries!
- not for WikiLeaks community

No more walls!

- filtering/blocking is condemned in faraway countries
- but also done here, and the technology is exported

Use our “freedom tools”

- Facebook, Twitter, Google etc are no tools for dissidents
- they were designed to make people traceable, and to develop (commercial) profiles
- very useful for dictators!

Underlying issue

- Western governments reserve the right to combat and block criminal online activities — to realize negative freedom
- The same applies to China (and others)
- But the Chinese have a slightly different concept of what criminal activities are
- This has nothing to do with technology! Hence it should not be discussed in those terms.
  • “must read”, debunking many cyber utopist myths and prejudices
• Now also NRC columnist
• Many presentation/documentaries available online, eg.
  • “Marriage from Hell” keynote at CCC 28 in Berlin at YouTube
  • At [TED.com](http://www.ted.com)
  • Featured in *Tegenlicht*, 26/9/11, at [uitzendinggemist.nl](http://www.uitzendinggemist.nl)
  • Or also with animations at [http://fora.tv](http://fora.tv)

---

**Conclusions**

• ICT-infrastructure needs more protection
  • the issues are real & threatening
  • awareness is a big issue, but also:
    • there are no commercial incentives to give people proper protection (think of Facebook, Android, etc)
    • can we defend what we are building? IT-scale down is very controversial (see voting machines)
• Public authorities can (must) be more assertive, eg.
  • companies that employ crappy security must clean up the mess themselves (and face penalties)
  • local/regional authorities lose their autonomy wrt. ICT
  • “Lektober” showed that they cannot handle IT-security
• You must read Morozov 😊