A Too Limited List of Infrastructures Identified as Critical

Yvo Desmedt

Department of Computer Science,

Florida State University, Tallahassee,Florida,

FL 32306-4530, USA, and

Royal Holloway, University of London, UK

desmedt@cs.fsu.edu,
http://www.cs.fsu.edu/~desmedt/

Overview

1) Introduction

2) The U.S. effort

3) Goal of the paper

4) Parameters of a simple attack

5) Agravating an attack

6) Sectors that has been overlooked

7) Recommendations

1. INTRODUCTION

WAR:

land(army) + sea(navy) → air(air force) → ABC

→ information warfare

information warfare: warnings ignored for many years

Different aspects were identified early on, such as:

- computer security,
- privacy,
- authenticity,
- reliability.

However: dependency on computers was only realized much later.

Examples of early warnings

- BBC documentary
- “some terrorist attack” e.g. mentioned in 1983 (called cyber terrorism today)

2. The US EFFORT

President’s Commission on Critical Infrastructure Protection

- created on July 5, 1996
- report delivered on October 28, 1997
- hearings by the Subcommittee on Technology of

  the House of Representatives.

input from scientists requested on February 26, 1998

Setup of agencies, e.g.

- Critical Infrastructure Assurance Office (http://www.ciao.ncr.gov/)
- the National Infrastructure Protection Center (FBI) (http://www.fbi.gov/nipc/index.html)

3. GOAL of THE PAPER

Has the report of the commission identified the major non-military potential targets of an information warfare?

If not one can waste resources.

The report is therefore critically analyzed.

4. Parameters of a simple attack

t_d time between the impact of an attack and the moment of detection

t_r time to recover from an attack after it has been detected

t_s time before an emergency stock of a supply, in general, a buffer, is exhausted

t_c a time of no return

f_q strategic and financial consequences that the attack will likely cause

f_c cost to perform the attack

Strategies of a potential enemy

- Doomsday strategy ($t_d + t_r > t_c + t_s$).

  Note: t_s may be secret.

- Undermining the (economic or military) potential

5. Agravating an attack

Attacker can:

- increase t_d (time to detect): after instead of destroy
- decrease t_s (time stock lasts): hack computerized warehouses + hack distribution and transportation
- increase t_r (time to repair):
  - hack computerized factories that make replacements
  - hack MANUAL (WWW)*
  - hack e-commerce*

* Worse impact in a society heavily dependent on the internet

6. Sectors that have been overlooked

General

- Sectors in which td is large
- mechanical sectors

Specific

- agricultural sector:
  - Microprocessor control equipment used to plant, fertilize, irrigate, spray pesticides, harvest, milk cows, food distribution to chickens, …
  - food distribution: as warehouses using bar codes
  - impact one may loose a full year. Worse if everybody uses same processor and/or same software.

- chip manufacturing industry:

  Heavily computerized.

  No human knows design of complete chip

  Examples:

  hack design of chip (e.g. using a target oriented virus/worm) to:

  destroy the working

  time bomb: affect many chips

  Society depends more on chips than on computers.

e.g.

Unintended destruction of memory chip manufacturers in Taiwan by Earthquake.

Even an old fashioned bomb may do serious harm the economy.

- Mechanical and manufacturing

  World is still heavily mechanical, e.g. appliances, construction equipment, transportation equipment.

  Attack can target:

  - design: CAD is often used. Potential Impact: faulty equipment
  - manufacturing itself: CAM, e.g. robots. Target: destructive or deteriorate
  - products themselves

- Pharmaceutical

  - production heavily computerized
  - R & D: of less medicines is heavily

    computerized

- weather prediction

  …

  …

  …

7. Recommendations

1. Include sectors as: warehouses, chip design and manufacturing, … … …
2. Make a list of future dependencies, e.g. digital libraries
3. Identify vulnerable sectors. Intelligence community: knows how and what to sabotage

Information warfare: knows about hacking

4. New laws: as industrial revolution: adapting laws too early/ late had dramatic consequences
5. Non-classified solutions to protect the many sectors on which we depend
6. Is easy to install software a blessing or a doom ?
7. Analyze the parameters (t_d, t_s, … … …) in more details
8. Add a new force. Air force is a consequence of airplanes.