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
Department of Mathematics, Royal Holloway, University of London, UK
desmedt@cs.fsu.edu, http://www.cs.fsu.edu/~desmedt/

Abstract

The report of the U.S. President's Commission on Critical Infrastructure Protection limited itself to those organizations for which a serious attack would have an immediate, visible impact, as well as to non-manufacturing areas of the economy. By doing so, it failed to address attacks whose impact only becomes visible after several weeks, and whose long term effect may be worse than the scenarios identified in the report.

We identify very critical areas to the economy that are heavily computerized. We explain how attacks can be mounted that will take a long time to detect, from which recovery will be slow, and that target those sectors that play the largest role in the economy and in the survival of the country. One should note that malicious code is not only able to shut down plants, airports, transportation, etc., but that it can also destroy plants.

A variant of a destructive attack will decrease the efficiency of a plant, which may be detected too late to prevent a company from going bankrupt. One can hack code in farming equipment employed to plant and maintain crops such that the plants never mature to grow fruits or seeds.

The unibomber has demonstrated that terrorists may have a PhD. A CAD expert can write a computer virus to modify chip design. Note that while bearings were the most critical component of a mechanical society, the chip is clearly the current one.

1 Introduction

The idea of a mechanical war is old. Indeed the idea of a war by land (army) or by sea (navy) is probably thousands of years old, if not older, and the concept of adding air (air force) is roughly a century old. The so called "non-conventional" weapons are not that new either. Chemical weapons go back to the beginning of this century; nuclear and biological weapons are more than 50 years old.

NATO has built extensive defensive and offensive capabilities to deal with these types of attacks. However, in the last 50 years, the economy, the military, the government, etc. have started to rely more and more on computers. Many warnings of the potential impact of a new type of war, nowadays called "information warfare" [3] have been ignored for many years. For example, the author and his former advisors warned already in 1983 [5, p. 257] against what they called "some terrorist attacks," now usually referred to as "cyber terrorism".

Targets (in particular since World War II) are not limited to military ones. Indeed destroying factories, transportation facilities, power plants, etc. may undermine the production of weapons, the transportation of troops, etc. The vulnerability of non-military targets in a war may determine the outcome of a conflict. Defending sectors critical to the survival of a country's economy, system, etc., is clearly a concern when planning the defense of a country or alliance of countries.

Lately, the U.S.A. has finally become more worried about the potential of information warfare and the impact of a strike against non-military targets. The President's Commission on Critical Infrastructure Protection was set up as a result.

It is natural to wonder whether the report of the President's Commission on Critical Infrastructure Protection has identified the major potential non-military targets of an information warfare. Indeed, if the report failed in this goal, then a defense set up to protect these sectors may be inadequate to protect the country or a group of countries such as NATO. For this reason, the report is critically analyzed, so that its shortcomings can be addressed by the U.S.A. and its NATO allies.

In Section 2 we discuss preliminaries, such as the complexity, the cost, and the destructive power of information warfare attacks against non-military tar-

gets. In Section 3 we discuss parameters that can be used when planning a cyber assault. In Section 4 we discuss how one can aggravate the impact of information warfare attacks and what the impact is of emerging technologies. In Section 5 we list the sectors of the economy that should also have been identified. In Section 6 we give some examples of such sectors. In Section 7 we briefly survey some of the technical means that can be used to carry out these attacks. We conclude with recommendations in Section 8.

2 Preliminaries

Before we start analyzing types of attacks and apply this knowledge to enlist infrastructures that should also be marked as critical, we make some preliminary remarks, which will be used later on in the text.

We briefly discuss a few topics.

2.1 Complexity of an attack

Although attacks by terrorists and computer hackers often use rather standard approaches, this is no reason to underestimate the complexity of a future attack. The unibomber has demonstrated that terrorists may have a PhD. Moreover, if information warfare is waged by a country one may expect a high level of sophistication.

2.2 Fall back strategy

Another general observation is that pseudo-experts often diminish the impact of information warfare saying that one can always go back to a paper-oriented mechanical society. This argument is flawed for several reasons. Indeed:

Computers automate, and so many companies have been able to downsize and reduce their workforce. The computer is carrying out many jobs that were done previously by humans. Since these humans have left, there are not enough people to fall back onto.

New technology often suppresses older ones, even if the older technology is more reliable or has other advantages. Indeed, the reliable and powerful Saturn V rocket (which placed a man on the moon, i.e. roughly 380,000 kilometers from earth) was replaced by the more expensive Space Shuttle (which can only travel to a few hundred kilometers from earth [9]). Also, commercial vacuum tube based radio sets are no longer produced, even though these are more resistant against EMP [10, 13] than the transistor based ones.

2.3 Cost and automation of an attack

In a mechanical society attacking several sites is more expensive than attacking a single one. Although the same airplane raid may be used to attack several sites, multiple bombs are needed.

The economics of information warfare are different. Indeed, computer viruses, for example, allow the automation of an attack. Although the current computer viruses are indiscriminatory [11], methods have been proposed to make computer viruses target a (range of) computer(s) and/or software applications [8] (see Section 7 for more technical details). So, the same siege can affect multiple targets at no extra cost to the assailant.

2.4 Destructive power of an attack

It may seem that information warfare at worst shuts down the application, or the computer. However, since computers are responsible for control functions, the damage can also be of a different nature. For example, many chemical products explode when at too high a temperature, and temperature control mechanisms are used to prevent such an event. However, as pointed out in [5, p. 257] these are computer controlled. So, by breaking in the computer one can change the temperature setting and have the chemical product that is being produced in a plant, or being stored, explode.

Many more examples will be given throughout the text, in particular in Section 4 and 6. See also Section 4.1 for a discussion on other types of impact of information warfare.

3 Optimizing a simple attack

To analyze the report, one first needs to find the parameters that are important in assessing how crucial a sector is. We first identify some of the parameters involved and then discuss their impact in details.

As we will discuss in Section 4, the attack can be aggravated when combining several simple attacks.

3.1 Parameters

We have as parameters:

- the time between the impact of an attack and the moment of detection of the attack, which we denote by t_d. Note that t_d can also be negative.

Indeed, if the attack involves some logical time bomb, the attack under way might be detected before it is set off.

- the time to recover from an attack after it has been detected, which we denote by t_r,
- the time before an emergency stock of a supply, in general, a buffer, is exhausted; we call this time t_s. Many systems have buffers, so that a union strike, or a natural disaster have limited impact. If the concept of buffer is not applicable, then $t_s = 0$.
- For truly critical systems, there is a time t_c of no return. For example, within a few days people die without having water. In general, from the moment a system has been successfully attacked, the damage caused by the attack will increase (in function of the time) until the system(s) is (are) sufficiently repaired or replaced.
- the strategic and financial consequences that the attack will likely cause, this can be expressed as a cost, however not necessarily expressed as a monetary value, which we denote as f_q,
- the cost to the organization (e.g., terrorists or country) to perform the attack, which we call f_c.

3.2 Strategies

We basically discuss two types of strategies. Note that a terrorist organization may not have the infrastructure or resources to follow a winning strategy. However, such an organization can still try to maximize the impact of an attack.

3.2.1 Doomsday strategy

If the time to detect plus the time to recover is larger than the critical time plus the time the emergency supply will last, i.e., $t_d + t_r > t_c + t_s$, then the terrorists or enemy country has succeeded in a doomsday attack. Otherwise, one can recover from the attack. So, one strategy for a potential enemy is to identify targets that permit a doomsday attack.

To evaluate t_d, t_r, t_c and t_s one can use control theory. Note that an in-depth analysis may be complex, since emergency measures can sometimes be introduced, such as rationing.

A defensive strategy might be to keep information about these parameters secret, as far as this is possible. In particular, the time the emergency stock will last can be kept secret. Therefore, an offensive strategy of this type will focus on sectors of the economy for which:

- the sum of the estimated t_d (the time to detect) plus the estimated t_r (the time to recover) is large, and
- the sum of the estimated t_c (the critical time) plus the estimated t_s (the time the stock lasts) is small.

It is important to notice that often the attacker can modify these parameters. Indeed:

t_d **can be increased** by using hiding mechanisms. These hiding mechanisms do not necessarily rely on computer techniques, as will be discussed in Section 4.1.

t_r **can be increased,** in particular when our society becomes even more computerized. Several offensive strategies to increase the time to recover what has been damaged will be discussed in Section 4.3.

t_s **can be decreased.** For example, when a stock is centrally managed, the distribution of the stock can be jeopardized using information warfare tactics. This will be discussed in Section 4.2.

The critical time (t_c) was not listed. Although it is obvious that when no food or water is available the time one can survive is smaller than if food, but no water is available. It is not clear what new impact a computerized society may have on decreasing t_c. A deeper study should however not overlook such a possibility (see recommendations in Section 8).

Even if the doomsday strategy fails, (so when $t_d + t_r \leq t_c + t_s$) the cost of recovering may have an undesired impact on the economy of a country. This aspect brings us to the second strategy.

3.2.2 Undermine the potential

Another strategy is to undermine the potential of another country, e.g., the economy or the military capacity. A foreign country, let us say, A succeeds if after the attack the assets of A are larger than those of country B. The assets of the offensive country will have diminished by f_c, and the ones of the defensive country by f_q. Clearly to evaluate how low the cost f_c can be, one evidently needs to assume that one knows the best method to perform the attack.

Evaluating f_c and f_q is not straightforward. When attacking (non-military) targets in a country, one will try to cause the largest impact on the outcome of the war. So, during World War II a high priority was given to bomb factories producing bearings (accordingly to the Webster dictionary, a bearing is a machine part in which another part (as a journal or pin)

turns or slides). Bearings were identified as being the most critical component in a mechanical society. Without bearings, there are no cars, trucks, railroad engines, (electrical) motors, therefore no airplanes, etc. So, bearings have an impact on several other industries. As such, a strike by an opponent limited to a certain sector can have a dramatic impact on many other sectors. Note that redundancy (such as redundant production facilities) may decrease the success of an attack. Recently the use of AND/OR graphs (a standard AI technique) has been suggested to evaluate f_c [6].

In Section 6.2 we will discuss which industry in the information age seems to play the role the bearings had in the mechanical world.

We first discuss how the attacker can modify some of the parameters.

4 Aggravating the impact

In a computerized society some of the parameters discussed in Section 3 can be modified by the attacker, aggravating the impact of the attack. We discuss some methods to achieve this result.

4.1 Increasing the time to detect

The typical strategy used in military and terrorist activities is to destroy the target. As already pointed out in 1983, instead of destroying a target, such as a chemical plant, one can "deteriorate slightly the performance of the overall system" [5, p. 257]. In a computerized world this attack is as feasible as one that destroys the target.

We now discuss the consequences of choosing a deteriorating-performance attack versus a destructive one. Let us take the example discussed in [5, p. 257]. Suppose that one modifies the control setting of a chemical plant. If these modifications imply an explosion, the attack (not including the delay of a logical time bomb) is detected immediately. So, the repair can start immediately. However, if the performance is deteriorated, it may take a while before it is detected. In the meanwhile, the company may have suffered a financial loss and may go bankrupt. Other uses of this strategy will be given and their consequences discussed in Section 6.

4.2 Decreasing the usefulness of a stock

Fuel, water and food are well known examples of material that is kept in stock. However, there are many more goods that have a stock. Software is kept in stock at the shop (or point of sale), the distributor, the vendor, etc. The same is true for cars, motors, controllers, etc. If the stock is large enough, but does not reach the needed, then the effectiveness of the stock is reduced.

In a traditional war, such stock can be bombed, the roads that are needed to transport the stock can be damaged, etc. We now discuss that similar and new methods can be used in an information society and discuss their impact. We should keep in mind that, as discussed in Section 2, new technology often replaces the older one. We identify, in particular, the following vulnerabilities:

Automated warehouses: Warehouses are more and more computerized and in some instances being fully automated. Bar code readers are usually the only part a customer sees of an automated inventory system (see also Section 6.1). The bar code readers enable the system to keep track of what is in stock. The system places automatic orders when the stock in the warehouse is running low.

Some warehouses uses robots to transport, to select, etc. the goods in the warehouse. These robots are computer controlled.

Tampering with such computerized systems may sabotage the proper distribution of goods that are critical.

Transportation and distribution: As indicated in the report of the President's Commission on Critical Infrastructure, transportation (in general) as well as gas and oil transportation are heavily computerized. For example, truck drivers are in contact with their base using cellular technology that rely on computers to keep track of the location of their vehicles, etc.

Moreover, the engines of modern cars and trucks are controlled by several computers. A logical time bomb planned well in advance may shut down modern cars as we discuss in Sections 6.2.

4.3 Increasing the time to repair

In a traditional war scenario the time to repair or replace parts that have been destroyed or damaged increases when similar strategies are used as those discussed in Section 4.2 and when the factories that make these parts have been bombed.

We now discuss that similar and new methods can be used in an information society and discuss their impact. We should keep in mind that, as discussed in

Section 2, new technology often replaces the old. We identify, in particular, the following vulnerabilities:

Digital libraries: More and more technicians and engineers rely on the World Wide Web (WWW) for repair manuals and specs (technical specifications). The WWW now has the same vulnerability as the library of Alexandria, which had several unique copies. The introduction of the printing press implied that many books are available at several libraries in the world, which increases the reliability and availability. The WWW is a return to the library of Alexandria model. Indeed, a WWW address corresponds to a single IP address [12]. So, a denial of service attack against such a server will delay access to potentially crucial information. The use of strategies such as mirror sites does not currently provide the multiplicity of copies usually available from traditional libraries. One should notice that we are currently in a transitional period in which WWW is replacing traditional libraries to an increasing extent. In the future the WWW may supersede the traditional format of library (see also Section 2).

Electronic commerce: Many observers believe that, although still in its infancy, electronic commerce has the potential to replace on a large scale our current way of commerce. In such a world availability of the servers will be very crucial. Denial of service may imply that orders of goods cannot be placed.

Automated warehouses were already discussed in Section 4.2. While the attack in Section 4.2 was aimed at diminishing the usefulness of an emergency stock, the aim described in this section is to delay repair. Let us clarify this with an example. After the destruction of fuel refineries, the emergency stock is fuel, while the tools needed for repair consists of pipes, controllers, etc.

Transportation issues were discussed in Section 4.2.

Note that such wide range services as we just discussed may be taken out by computer viruses (see also Section 2).

5 Type of sectors that should have been identified

Although we kept the analysis in Section 3 rather simple, the importance of the parameters enumerated allows us to analyze the report by the President's Commission on Critical Infrastructure.

5.1 Sectors that were identified

The report of the President's Commission on Critical Infrastructure Protection (http://www.pccip.gov) identified the following areas as critical:

1. Information and Communications,
2. Electrical Power Systems,
3. Gas and Oil Transportation and Storage,
4. Banking and Finance,
5. Transportation,
6. Water Supply Systems,
7. Emergency Services, and
8. Government Services.

It is not clear how these sectors have been chosen. Considering the parameters discussed in Section 3 and the strategies to aggravate the attack (see Section 4) one observes that:

- many attacks on these sectors would have an immediately visible impact, i.e., $t_d \leq 0$. To be more precise, although a logical time bomb could be used to delay the impact of an attack, the sectors identified have the feature that once an attack is activated, the attack will likely be detected soon.
- all address current applications of computers.

One can also make the observation that:

- all areas identified are non-manufacturing sectors of the economy.

5.2 Overlooked

By focusing on sectors falling in the above categories, the report has overlooked:

1. those areas of our society that are vulnerable to attacks whose impact may only become visible after several weeks, or even months, i.e., that have a large to very large t_d,
2. how emerging and new applications will make us even more dependent on computers,
3. the mechanical sectors of the economy.

We now list some examples of sectors that should have been identified. Since, Item 2 was already discussed in Section 4.3 we do not list such sectors. We therefore focus on sectors with long term vulnerabilities that may be worse than the scenarios identified in the report of the President's Commission on Critical Infrastructure.

6 Sectors that are currently vulnerable

In Section 4.1 we discussed that an attack that does not destroy production facilities but decreases their efficiency may be harder to detect. We apply this to a few sectors in more details. We discuss in Section 7 the technical aspects of how to undermine the sectors surveyed in this section.

6.1 The agricultural sector

Farming is becoming more and more computerized. Microprocessors (see Section 7 for a technical description on how to attack these microprocessors) and/or computers control equipment used to:

- plant crops,
- fertilize,
- irrigate,
- spray pesticides,
- harvest,
- milk cows (see, e.g. [14]),
- food distribution to chickens,
- ...

Also the food processing industry and distribution of food depends heavily on computers. For example, supermarkets use bar code readers to keep track of their stock in a similar way as warehouses do (see Section 4.2 for more details).

The use of faulty equipment (machinery and computers) may imply crops that have been poorly planted, have not received the appropriate amount of irrigated water, fertilizer, etc. Such a crop may provide a smaller yield. It is likely that such a reduced yield would be detected too late. For some plants and regions of the world with cold winters, detecting a reduced yield one month after planting may be too late to recover from for a whole year. If sufficiently many producers of farming equipment fell victim to such an attack, the damage could have disastrous dimensions.

In [14] is mentioned that:

> If the milking equipment can't operate for just two days, many of the cows could get sick or even die.

Another example is chicken farms. Microprocessors do not only distribute the food to the chicken, but also turn on and off the lights. It is obvious that there are many more examples of the use of microprocessors and computers in the agricultural sector.

6.2 Chip manufacturing industry

This industry is quite computerized, and therefore very vulnerable to well planned attacks. CAD (Computer Aided Design) is utilized to design electronic chips. The manufacturing of chips is also heavily computerized. Only the computer "knows" a chip under production. Many modern chips have so many transistors that no single human knows the entire design. Indeed, the Pentium chip contains millions of gates. We survey in Section 7 the technical details of mounting such an attack.

We discuss the impact of two types of attacks in which a hacker alters the design of a chip. In a

destructive attack the chips produced will malfunction completely. Such an attack will be detected rather soon.

delayed attack, discussed by the author in 1986 [7], the chips will usually behave as specified. However, a triggering mechanism may activate a part of the chip designed by the hacker. This triggering mechanism can be activated by a logical time bomb, a random event, a password, etc. If a password is used, one may discover it when reverse engineering the chip. Often one can then use filter techniques (hardware or software) that block such a password to ever reach the chip. However, if a digital signature is needed to activate the Trojan Horse [2, 11], no counter measure would work but to replace all the affected chips.

As pointed out by the author in 1986 [7, p. 461]:

> Chips are used today in telecommunication systems, instruments, controllers (e.g. controlling the temperature of a process in a chemical plant), consumer electronics, security systems (e.g. detecting burglary), medical electronics, industrial electronics (as in robots), cameras, cars, trains, aviation, military applications, space and so on.

To further illustrate this, note that many cars contain so many chips that the average driver is no longer able to maintain his car. So, it seems that we can conclude that *our society depends even more on electronic chip technology than it does on computers.* A widespread attack will have unforeseeable, disastrous consequences. An example is the use of time bombs that make chips fail at the same time (for more examples consult [7]).

6.3 Mechanical manufacturing sectors

Even if we move more and more to an information society, we still rely heavily on mechanics. Examples are found in the following sectors:

Appliances Airconditioners, dryers, refrigators, washers, etc. are heavily used in our society.

Construction Cranes and earthmovers are examples of mechanical tools used to construct buildings and roads.

Transportation Airplanes, cars, elevators, trucks, and trains, are all mechanical.

...

There are three fronts on which one can wage an attack. One can target:

the design of these products. Many mechanical tools are designed using CAD. An impact of attacking CADs is that faulty equipment may be produced.

the manufacturing of these products. The plants that produce these are extremely computerized. Computer Aided Manufacturing (CAM) [1] is a very common technique. For example, robots, controlled by computers, play a key role in a car manufacturing plant. One should also remark that the mechanical manufacturing sector is extremely interconnected. This implies that attacking a small fraction of the sector may have a large ripple through effect. For example, a union strike in one sector often implies that other factories have to shut down. The same is therefore true for a cyber attack. A cyber attack could be:

destructive, and sabotage the production facility, or only

deteriorate the products produced.

Indeed, for example, tampering with the computers that control the robots in a plant may not only sabotage a production line, but produce faulty products, e.g., the robot may be programmed not to squeeze screws tight enough. The goal of the attack could also be to reduce the yield of the production process.

the products themselves. Microprocessors can be modified by cyber attacks while being designed, as discussed in Section 6.2 (see Section 7 for more technical details).

6.4 Pharmaceutical industry

While emergency services are included in the report of the President's Commission on Critical Infrastructure, the pharmaceutical industry is not.

In the western world, many people take medical drugs rather regularly. As in the mechanical and chemical world, the production of these medicines is heavily computerized, so production can be sabotaged. Moreover, the research on what chemical components should be selected depends heavily on computers. Robots have automated to a large extent several tests that used to be done by humans. Statistics on medical tests are evaluated by computers. So, although such an attack seems farfetched and has to be planned several years before it has an impact on society, it is not excluded that one may succeed.

7 Technical aspects

Many techniques for attacking computers are well known, such as Trojan Horses, computer viruses, logical time bombs, etc. Since it usually believed that the internet has no impact on the safety of the chips (for example used in cars) we focus on this aspect.

Hardware viruses [7] and their more general variant, called target oriented viruses [8], were first described by the author. As normal computer viruses, they can be hidden in a computer game, electronic document, etc. This type of computer virus will behave as almost-benign. Only when the computer virus detects that it has infected a target will it switch on a delayed "illness phase." Computers/programs that are not targeted will have no symptoms of illness. So, the computer virus spreads through them without causing any harm. In the case of a hardware virus, the target is a CAD program. We now explain in more details how the targeting works.

When targeting a computer or a user, one can use the IP address, or the user's name, etc. When targeting a specific program one can use the concept of "signatures" [11] (not to be confused with digital

signatures). A program can be identified, for example, by some sequence of code lines (or sequence of machine instructions) unique to that program. Currently, "signatures" are used to defend against computer viruses by identifying the presence of a known one. However, target oriented viruses use this as an offensive tool. The signature of the target program identifies the program in which to trigger the delayed illness phase. So, anybody (e.g. a student) using a CAD program can easily write a signature of that CAD program.

We now continue explaining how the virus proceeds. After a while the virus removes itself from all computers/program except those that it targeted and stops spreading (it may even remove its viral part of its program). The remaining computer "viruses" (technically, they are no longer viruses) cause a specific harm, such as modifying the design of a machinery, electronic chip, etc. This symptom is limited to those targets identified by that signature.

So, one can conclude that although it seems that electronic chips are not networked and therefore not vulnerable to internet type of attacks, the software that was used to design them was often developed on internet connected machines. So, computer chips were virtually connected to the internet during their design. A similar comment applies to advanced manufacturing equipment.

Further details, such as how to make the virus harder to detect, are discussed in [7, 8].

8 Recommendations

Some sectors others than those on the list of the President's Commission on Critical Infrastructure have been discussed in this paper. In particular, the ones that are currently critical were discussed in Sections 4.2 and 6, while those that are emerging as critical in Section 4.3. It is clear that these lists are not exclusive.

The fact that the sectors we identified are not on the list of the President's Commission on Critical Infrastructure seems to indicate that the selection of the sectors involved was done in a hasty way. We therefore discuss how one can learn from the mistakes and suggest which steps can be taken to come to a more complete picture. We recommend that:

1. the following sectors be included in a future list:
   - automated warehouses,
   - chip design and manufacturing,
   - food production, processing and distribution,
   - design and manufacturing of mechanical products,
   - the pharmaceutical industry.
2. a separate list be made of sectors that are emerging as critical, such as:
   - digital libraries, and
   - electronic commerce.
3. a serious effort be made at identifying all sectors of our society that are sufficiently critical and that are vulnerable to information warfare. The intelligence community knows how to sabotage a country using traditional means. Some sectors, such as those that are not sufficiently computerized, are not directly vulnerable to a cyber attack. However, as we discussed, new strategies and new forms of attacks are possible due to the specific nature and impact of computers. A collaboration between the intelligence community and information warfare experts should identify, in a classified study, which sectors of our society should really be included in the list of critical infrastructures.
4. new laws be adapted to enforce availability, reliability and security. As in the aviation, car-manufactoring, medical community, (etc.) companies should be made responsible for their computer (hardware and software) products. Although the internet is an emerging technology, at some stage new laws will be required to avoid chaos. Countries that during the industrial revolution gave appropriate rights and duties to all parties involved benefited enormously. Those that did not adapt their laws at the right moment suffered revolutions with long lasting effects. There is no reason why the information revolution will be different. Identifying which laws should be adapted at what moment is the difficult question.
5. non-classified solutions be worked out. Since computers are used in so many more critical sectors than the report identified, one may not be able to limit the industries and sectors to be included. It is therefore also questionable whether the government can play a leading technical role. Since the problem is so widespread, non-classified solutions must eventually be worked out.
6. to seriously analyze whether the concept of "easy to install software" is a blessing or a doom.

When new software can easily be installed, one can install Trojan Horses and computer viruses can spread widely.

7. to analyze the parameters we discussed in more details, in particular whether t_c (the time critical to survive) can be decreased using new methods.

Other and more detailed recommendations have been given by the author in [4]

References

[1] T.-C. Chang, R. A. Wysk, and H.-P. Wang. *Computer-Aided Manufacturing*. Prentice Hall, Englewood Cliffs, N.J., second edition, 1997.

[2] D. E. R. Denning. *Cryptography and Data Security*. Addison-Wesley, Reading, MA, 1982.

[3] D. E. R. Denning. *Information Warfare and Security*. Addison-Wesley, Reading, MA, 1998.

[4] Y. Desmedt. Viewpoint on research and development needed to achieve survivability of the critical information infrastructure. In *Position papers for the 1998 Information Survivability Workshop, participants' edition*, pp. 57–61. IEEE Computer Society, October 28–30, 1998. Orlando, Florida.

[5] Y. Desmedt, J. Vandewalle, and R. Govaerts. Cryptography protects information against several frauds. In *Proc. Intern. Carnahan Conference on Security Technology*, pp. 255–259, Zürich, Switzerland, October 4–6, 1983. IEEE.

[6] Y. Desmedt and Y. Wang. Maximum flows & critical vertices in and/or graphs. Presented at INFORMS (INstitute For Operations Research and the Management Sciences), Cincinnati, Ohio, May 2-May 5, 1999.

[7] Y. Desmedt. Is there an ultimate use of cryptography? In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto '86 (Lecture Notes in Computer Science 263)*, pp. 459–463. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.

[8] Y. Desmedt. The next generation of computer threats. In D. Lefkon, editor, *Safe Computing, Proceedings: Fourth Annual Computer Virus & Security Conference*, pp. 596–607. DPMA and ACM-SIGSAC and IEEE-CS, March 14–15, 1991.

[9] Encyclopedia of science & technology. McGraw-Hill, New York, 1992.

[10] E. J. Lerner. Electromagnetic pulses: potential crippler. *IEEE Spectrum*, 18(5), pp. 41–46, May 1981.

[11] C. P. Pfleeger. *Security in Computing*. Prentice-Hall, Englewood Cliffs, New Jersey, second edition, 1997.

[12] A. S. Tanenbaum. *Computer Networks*. Prentice Hall, Englewood, New Jersey, third edition, 1996.

[13] E. Teller. Electromagnetic pulses from nuclear explosions. *IEEE Spectrum*, p. 65, October 1982.

[14] Will Y2K bug stop flow of milk? http://cnn.com/TECH/computing/9903/25/foodchain.y2k.hln/index.html

Note

An earlier version of this text was sent, on March 5, 1998, to Terry Mayfield, Institute For Defense Analyses. Its title was: "The limited number of areas identified as critical and its potential impact on a well planned attack on the computer infrastructure in the U.S.A." This was a response to his request on February 26, 1998 for R&D viewpoints from academics to help the President's Commission on Critical Infrastructure Protection (PCCIP) Transition Office.

This research was done while the author was at the University of Wisconsin – Milwaukee.

Copyright