How to prepare for the next waves of Information Assurance issues?

Eric A.M. Luiijf

Clingendael Centre for Strategic Studies (CCSS),
TNO Defence, Security and Safety
P.O. Box 96864, 2509 JG The Hague
The Netherlands
eric.luiijf@tno.nl

Abstract: L'histore se répète. In general, each development wave of new technology shows a lack of security. The same lack of security can be found in the area of information and communications technology resulting in a lack of Critical Information Infrastructure (CII) Assurance. By looking back, we can predict the upcoming operational and maintenance issues in critical information infrastructure assurance. Organisational, manufacturing, awareness, educational, and technical threats and related information assurance gaps can be predicted. What are the information assurance challenges to avoid a failure of the CII?

Keywords: Critical infrastructure, critical information infrastructure, dependency, protection.

1 Introduction

Modern societies are increasingly dependent on a set of products and services which comprise their critical infrastructure (CI). In most cases, the CI depends on information infrastructures which in turn may be critical to the operation of the CI. Such critical information infrastructures (CII) comprise processors, computers, local networks, and communication technology components. Critical Information Infrastructure Assurance should provide the protection society at large expects and requires.

In section 1.1, we define some terms. The next section discusses the current Critical Information Infrastructures and a high level discussion on Information Assurance for CII. In section 3, we show that the development cycles of technologies in general show a lack of security in the first development waves. The difference with other technologies is that information and communication technology (ICT) itself provides the cheap means to distribute attack knowledge, the attack tools and the attacks themselves. In section 4, we will look at some historic examples of reoccurring IA-failures. As “l'histore se répète”, we can predict the next failures in Critical Information Infrastructure Assurance given

Euro-Atlantic Symposium on Critical Information Infrastructure Assurance
23-24 March, 2006 Riva San Vitale, Switzerland

current and predicted ICT-developments. From that, we can derive the assurance issues for the next generation of the CIIs, e.g. when a manifold of processors in cloths, cars, house appliances etceteras are connected to the ambient critical information infrastructures.

1.1 Definitions

A *critical infrastructure* (CI) consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments (from: [Eu04a]).

A *critical information infrastructure* (CII) consists of those information and communication technology facilities, networks, services and assets which, if disrupted or destroyed, either (1) have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments, or (2) causes the functioning of a critical infrastructure which it supports to be seriously disrupted.

A *critical infrastructure product or service* is a product or service which is the end product of a *critical (information) infrastructure* (from: [LNK03]).

A *critical sector* comprises a set of *critical infrastructure products and services* which are addressed as a common governmental and/or private responsibility.

Dependency is either a link or a connection between two products or services, through which the state of one influences or correlates to the state of the other. *Interdependency* is the mutual dependency of products or services (from: [Ac03]).

2 Critical Information Infrastructure Assurance

2.1 Critical Information Infrastructures

When looking at the definition of Critical Information Infrastructure (CII), it is clear that CII either comprises those information and communication technology (ICT) based infrastructures that are essential for a Critical Infrastructure or a ICT-based infrastructure that is a critical infrastructure on its own.

The first type of critical information infrastructures include:

- air traffic control systems,
- navigation and precise timing systems (e.g., GPS, Galileo),
- logistic and ordering systems for food and medicine distribution,
- health care databases,
- the critical supporting ICT-infrastructure for first responders,
- process control systems in the energy sector (power, gas, and oil),

- process control systems that control the processing and transport of drinking water and of waste water,
- process control systems that control pumps, valves, and locks to regulate water levels,
- process control systems in food and medicine production,
- process control systems in rail systems,
- tunnel management systems,
- process control systems in chemical and nuclear plants.

The second type of critical information infrastructures include:

- the ICT-components that control the critical telecommunication infrastructure (e.g., name services, routing/switching, location registers, Internet exchanges),
- the ICT-components of the critical financial services (e.g., the ATM-infrastructure, the SWIFT-financial clearing infrastructure, exchanges).

Dependencies of CII stem for example from:

- interconnected critical infrastructure, e.g. power production control systems which deliver information to the business network which is connected with the power exchange market,
- the use of "global" Internet as information carrier,
- the use of common, often commercial-off-the-shelf, ICT products with their inherent vulnerabilities, e.g. operating systems, routers, telephone branch exchanges,
- converged communication services and links.

2.2 Critical Information Infrastructure Assurance

Assurance of Critical Information Infrastructure comprises the integrated set of security organisation, personnel security, physical security, communication/transmission security, electro-magnetic security, and – last but not least – information security. When discussing Critical Information Infrastructure Assurance one needs to take the full and integrated gamut into account.

To reduce the complexity, one needs to look at the various development phases of Critical Information Infrastructure Assurance (design, implementation, and operational) as well as the level of application (organisation, capability, technical). The organisational phase comprise the full operational life cycle of the CII and its components. Technical is used here in an wide sense, it includes for instance policy measures. Together they form a three-by-three matrix of activity areas:

- the design phase – **organisational** area of the assurance includes for instance high level assurance policy definition, the architectural design of the assurance system for the CII, and strategic planning for assurance education,
- the implementation phase – organisational area includes for instance public-private governance, assurance implementation planning, and integrated risk assessment, and the development of an assurance education curriculum,

- the operational phase – organisational area includes for instance policy compliance verification, dynamic risk assessment taking care of the dynamic threats to the CII, and maintenance policy,

- the design phase – **capability** area includes the design of the required assurance capabilities, e.g. the design of base levels of assurance measures for multiple threat environments,
- the implementation phase – capability area includes for instance information sharing capabilities for public-private governance,
- the operational phase – capability area includes for instance capabilities for an integrated capability for identification and authentication which gives access to authorised persons to ICT means and physical areas,

- the design phase – **technical** area includes the design of technical solutions for improving the assurance of CII,
- the implementation phase – technical area includes for instance security technology development and the development of regulatory and policy measures,
- the operational phase – technical area includes for instance quality monitoring and control of assurance measures, technical measures (e.g., access control, identification and authentication, patching, audit, shielding, cryptographic devices, vetting of personnel, secure disposal of old equipment and information containers).

Basically, security should start at the top left box "design phase/organisational area" as the assurance policy should match the needs for an assured service level of the critical infrastructure and thus the underlying critical information infrastructure. The reality, however, is that the current or "IST" situation shows a large neglect for security in the design phase. Most of the time, security is added as an afterthought resulting in a patch work of sometimes unrelated or even conflicting measures from the various assurance dimensions.

The requirements for the capabilities and underlying technical aspects come from the high-level assurance policy for the CII (design phase – organisational area) and will result in a set of assurance measures in the operational phase – technical area.

3 Technology developments and Assurance

When looking back at development cycles of technologies, generally new features are developed without taking much care of the assurance aspects. Only after severe incidents, security and safety measures are added to the technology. Some examples:

- independent inspections after many exploding steam boilers,
- block control system for railways,
- electrical fuses,
- lower oxygen levels in Apollo spacecraft,

- pilot eject seats in fighter aircraft,
- regulatory measures for sea-going and river vessels,
- flight levels and air control.

In information and communication technology we can recognise the same struggle. Security is not built in upfront when new technology is developed. Unfortunately, this is still the case. We only have to look at new ICT appearing on the market or the "prototypes" of new ICT-based services developed without any assurance under research grants by nations and the EU.

The same phenomena can be recognised in ICT. We do not learn from earlier assurance problems in the relative young ICT history. The aircraft industry has done better. Should we use this historic technology development phenomenon as excuse? What makes it worse is that ICT provides the cheap means to distribute attack knowledge, the attack tools and the attacks themselves.

4 L'histore se répète or can we break the cycle?

Within the ICT-sector, and thus in the technologies that support our critical information infrastructures, one can recognise the reoccurrence of the same assurance problems over and over again. It looks like that new hardware and software lines need to rediscover earlier failures. We will discuss a set of examples and suggest some solutions:

1. Assurance policies
   New CII services require aligned assurance policies. Especially, when critical information infrastructures are coupled to create new critical end-to-end services, policy misalignments on the one hand and late policy development and implementation on the other hand create gaping holes for criminals and others. Over and over again, the dynamics of ICT in the CII and the late development of law enforcement policies and legal support seem to surprise society. The solution is that there is a need for dynamic assurance frameworks for interconnecting CIIs and pro-active development of law enforcement policies, methodologies, and tools (e.g., inforensics). One can predict that the dynamics of UMTS, RFIDs, Eagle/GPRS in cars, and smart clothing, so on will show failure of pro-active policy development by governments and law enforcement.

2. New ICT replaces "old automation".
   When new ICT is introduced as replacement for old technology, this often occurs in a silent fashion. The introduction to the system management people does not include security aspects. The systems are installed by the manufacturer out-of-the-box without changing default passwords, removing unwanted and unnecessary functionality, etcetera. An example is the old Private Branch Exchanges (PBXs). The "head of the cleaning services" had learned how to rewire an internal phone extension when needed. He could set of remove some functions like direct external

access in a clumsy manner. The new PBX is operated from a terminal. That the system contains a commercial-of-the-shelf operating system (e.g., Windows), had open access to the outside world via a standard built-in modem, and could be misused became only obvious after a couple of months when very high bills appeared.
We can predict that the same learning curve will appear with VOIP where wrong (partially default) configurations will lead to costly redirected phone traffic and external network break-ins. The same can be expected with in-car systems, domotics, car-traffic management systems, … External manipulation of building management systems and process control systems in CII has already been reported. The latter will become a major cause of CII break-downs pretty soon unless the appropriate assurances are applied by industry: deny-all as out-of-the-box default, no default accesses, proper training and education of system managers.

3. Limited CPU power in new technology
   New waves of microprocessors have limited processing power, thus appropriate security measures are not applied, e.g. crypto. Examples of lack of security can be found in the initial generations of mobile phones, process control systems, bank cards. The next waves will be the taking over of new generations personal assistants, on-person health systems, and unauthorised manipulation of car - traffic manipulation systems. The Japanese and Australian emergency management centres have experienced denial-of-service problems due to a Trojan game. The solution would be to wait until the security is at an appropriate level. As that is an utopia, manufacturers should be required to publish the security risk and should be required to built a critical information infrastructure protection mechanism (e.g., a smart filter for a UMTS Base Station Controller).

4. Distrust in CII
   Users will distrust ICT and therefore CII services, especially financial services, if a major phishing or Trojan attack takes place. Such an attack is still relatively easy due to low software quality resulting in many security vulnerabilities and users lacking proper security awareness that users are easy to lure into security traps. The solutions require a manifold of actions: liability for bad software, co-operative international actions by law enforcement, awareness education of “all” users.

5. Buffer overflows
   In 1978, we removed all 50+ buffer overflows in a mainframe operating system. According to CERT/CC, currently most vulnerabilities in operating systems and application software are due to buffer overflows. We almost can predict that around 2050 the global CII fails due to an exploited buffer overflow causing a total collapse of the global CII causing 1000s of dead people, millions of people wounded, an economic dawn and a total chaos with governments out of control. Or?
   Why have we not trained the last five or six generations of programmers about information assurance from the start on? Why did we loose the strong typing concepts from Algol’68 and ADA? Despite some intermediate solutions like traps in some operating systems and some hardware checking, can we develop a successor of C(++) and JAVA which by built-in design concepts definitively

removes all possibilities for buffer overflows? If a software manufacturer has not taken care of buffer overflow protection, he should be automatically liable for all disturbances to the CII which may result from that.

6. Input validation
   As I learned in 1974, in my early days of programming of punch card systems, strong input validation is a necessity. We validated all field of the card for expected input and matched expected combinations. Invalid cards had to be rejected.
   Current protocols and many programs presume a co-operative environment in which no wrong protocol packets or intentional actions to break a protocol or program take place. As example, it has been reported that process control systems are pretty weak in validation of protocol elements. The result may be a CII crash. The solution is that weak protocols need to be redefined in a way which excludes all not valid protocol elements. Software manufacturer should be automatically liable for all disturbances to the CII which may result from not appropriate validation of protocol elements and inputs.

7. Bioterrorism in Cyberspace
   New technology waves neglect earlier "bioterrorism in Cyberspace". As an example, new mobile phones and PDAs are vulnerable to viruses, worms, and Trojan horses. One can expect that the next generation of worms and Trojan horse code will attack the network of processors in cars and trucks. Currently, a mid-size car contains over fifty processors some of which are connected to a "board net". The amount of processors per car or truck increases fast with each new generation, and the vehicles will soon communicate with external networks including the internet. Starting 2007, European car manufacturers expect to build in all new cars an Eagle (automatic GSM alert in case of a car collision) and GPRS. A virus, worm, or Trojan code penetrating the 'board net' may lead to dangerous behaviour, e.g., unexpected braking or acceleration; all air bags blown on a high-way, etc. To protect the critical transport infrastructure, new developments in the supporting information infrastructure are required which disrupt by design the spread of hostile code and develop "software fuses" that disrupt the spreading means.

5 Recommendations and Conclusions

When assessing Critical Information Infrastructure Assurance, one needs to understand the different areas of the 'playing field': from organisational – design to technical – operations. One also needs to understand the broad gamut of protection and security areas which need to be integrated and combined to provide the appropriate assurance of CII.

Critical Information Infrastructure Assurance for both current and next generation infrastructures should take a careful look at previous assurance failures. As we have shown, one can predict the upcoming assurance issues in next generations of CII. Or

will we be able to break the historic cycles and start with security as part of the critical information assurance design?

References

[Ac03] ACIP consortium: Analysis and Assessment for Critical Infrastructure Protection (ACIP) final report. EU/IST, Brussels, Belgium, 2003.

[BDB05] Bruce, R.; Dynes, S.; Brechbuhl, H.; Brown, B.; Goetz, E.; Verhoest, P.; Luiijf, E.; Helmus, S.: International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues. TNO report 33680, TNO Information and Communication Technology, Netherlands & Tuck School of Business/Center for Digital Strategies at Dartmouth, USA, July 2005.

[Eu04a] EU: Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702 final. Communication from the Commission to the Council and the European Parliament, Brussels, 2004.

[LNK03] Luiijf, H.A.M.; Nieuwenhuijs, A.H.; Kernkamp, A.C.; de Jong, K.Y.; Burger, H.H.; Bik, A.L.L.C.M.; Hoogstraten, J.M.: Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten. [Critical Infrastructure Protection: Quick-scan of critical products and services]. TNO-report FEL-03-C002, The Hague, The Netherlands, 2003.

Biographical Notes

Eric Luiijf M.Sc(Eng) obtained his Masters degree in Mathematics at the Technical University Delft in 1975. After his duties as officer in the Royal Netherlands Navy, he joined the Netherlands Organisation for Applied Research TNO. Eric is currently employed by TNO and the Clingendael/TNO Centre for Strategic Studies (CCSS) as Principal Consultant Information Operations and Critical Infrastructure Protection. Eric's experience in information security and information assurance is broad: as systems programmer, infosec manager, researcher, and security policy developer. As the Dutch national technical representative, he contributes to several NATO working groups on information assurance. Regarding critical (information) infrastructure protection (C(I)IP), he was the lead author of the essay 'Bitbreuk' (In Bits and Pieces' (2000)) and one of the two main researchers of the KWINT study which looked at the vulnerability of the Dutch part of Internet (2001). From 2002 on, Eric is the R&D leader in a sequence of critical (information) infrastructure projects commissioned by the Dutch Ministries of the Interior, of Transport, Public Works and Water Management, and of Economic Affairs. These projects are part of the Dutch Critical Infrastructure Protection programme "Bescherming Vitale Infrastructuur", which includes the organisational, physical protection and information assurance efforts of all critical sectors. Eric is work package leader in several European IST and PASR C(I)IP projects: VITA, CI^{2}RCO, and IRRIIS. Eric is a editor of the European CIIP newsletter, member of EWICS and of the NATO/EAPC Civil Emergency Planning/ Critical Infrastructure Protection working group. He was interviewed many times by national and international newspapers, monthly publications, radio and national TV on topics like information operations ("Cyber warfare") and information security. He has published many popular articles as well as scientific publications.