5 Vulnerability Assessment

Vulnerability can be defined as susceptibility to injury or attack. It can be defined in the context of CIP/CIIP as "a characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat".[85] Considering limited, technical subsystems, vulnerabilities may be seen as "flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy".[86]

What is Vulnerability Assessment?

Vulnerability assessment is often seen as a single step in the overall risk analysis methodology. It is about the systematic examination of critical infrastructure, and the interconnected systems on which it relies (including information and products) to identify those critical infrastructures or related components that may be at risk from an attack, and to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.[87]

Assessing the vulnerabilities of a relatively restricted IT system such as a business network is far easier than doing the same on a higher system level. There are numerous vulnerability assessment tools that scan operating systems and applications for potential problems.

However, it may well be that vulnerabilities and infrastructure disruptions will not be traceable in any useful way to single technical subsystems – this could be due to a consequence of a overwhelming system complexity.[88] The

85 President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures* (Washington, October 1997), Appendix, B-3.

86 Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800–30 (Washington, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, p. 15.

87 President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures* (Washington, October 1997), Appendix, B-3.

88 Westrin, Peter. "Critical Information Infrastructure Protection", in: Wenger, Andreas (ed.), *The Internet and the Changing Face of International Relations and Security*. Information & Security: An International Journal, Volume 7 (2001), pp. 67–79.

analysis of vulnerability should therefore be based instead on *functional units*, whose interactions with each other and with their environment can best be described by way of their societal manifestations as a whole, with less emphasis placed on technical issues.[89]

Additionally, threats and vulnerabilities must be seen as two sides of the same coin: As a threat-source does not present a risk when there is no vulnerability that can be exercised, a vulnerability on its own also does not represent a risk when there is no threat. Besides, especially when considering human threats, for example terrorism, a sole focus on vulnerabilities, sensible though it may be with respect to cost-benefit arguments, often implicitly assumes that terrorist actors will also recognize and identify the same infrastructures as priority targets – an assumption which might backfire.[90]

Examples of Vulnerability Assessments

There is a lot of emphasis on vulnerabilities in the current CIP/CIIP debate, resulting in variety of vulnerability assessment methods and tools. However, they vary considerably in terms of the size and nature of the system they can evaluate. Below, the following five examples are described:

- Example 1 (Australia) – PreDict Vulnerability Assessment Process (PreDict)
- Example 2 (Germany) – Vulnerability Assessment CYTEX 200x (CYTEX)
- Example 3 (Netherlands) – KWINT Vulnerability Assessment (KWINT)
- Example 4 (United States) – DoE Vulnerability Assessment Methodology (DoE)
- Example 5 (United States) – CIAO Vulnerability Assessment Process/Project Matrix (CIAO)

89 Ibid.

90 Zimmermann, Doron. *The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception*, ed. Andreas Wenger, *Züricher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 67* (Zurich, 2003), pp. 61–65.

Example 1 (Australia) – PreDict Vulnerability Assessment Process (PreDict)

♦ The PreDict approach also appears in *Chapter 1: Sector Analysis* and in *Chapter 2: Interdependency Analysis.*

In 1998, Australian government officials decided to analyze the national defense-related infrastructure in order to develop strategies to remove, ameliorate, and avoid identified vulnerabilities. A multi-step →*Vulnerability Assessment* Process was developed for this project (Figure 24).[91]

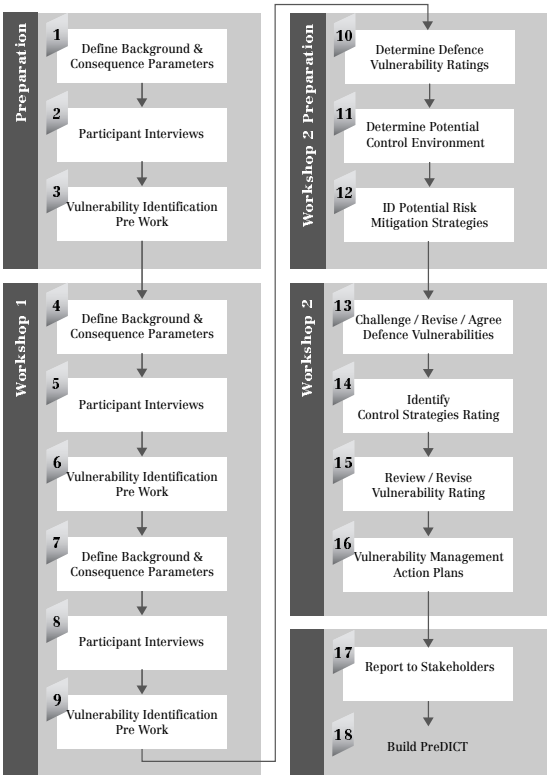

Figure 24: PreDict Vulnerability Assessment Process

In the first phase, the study identified vulnerabilities in fifteen infrastructure sectors and highlighted their interdependence. In a second phase, the project identified preliminary strategies aimed at removing the vulnerabilities, with a special focus on defense needs.

In a next step, industry *Vulnerability Profiles* were developed for each of the ten sectors, based on industry analysis and interviews, with a focus on the critical interdependencies between them. The vulnerabilities were grouped into twelve "Broad Risk Areas" in order to compare and contrast vulnerabilities between industry sectors and defense, and to group the identified vulnerabilities into common

91 KPMG / National Support Staff. *Predict Defence Infrastructure Core Requirements Tool* (PreDICT). http://www.defence.gov.au/predict/general/predict_fs.htm.

areas for analysis. The majority of the Broad Risk Area titles were drawn from →*Sector Analysis* (PEST, Porter's analysis, and SWOT analysis).[92]

The vulnerabilities were rated first by quantifying the consequence of each vulnerability by degree (→*Categories*: "insignificant", "minor", "moderate", "major", "catastrophic"), and then by determining the likelihood of the occurrence of the vulnerability. The vulnerability rankings for each Broad Risk Area were calculated using a →*Vulnerability Rating Table* and were visually represented on a →*Vulnerability Profile Chart* (Figure 25):

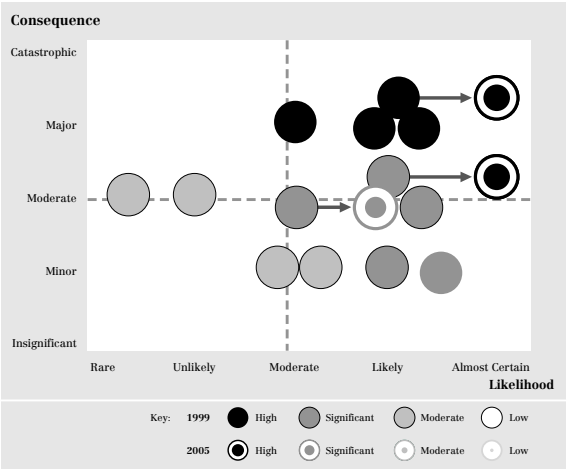

Figure 25: Vulnerability Profile for the Technology Sector

Vulnerabilities with the highest rating by sector using this method were prioritized for the development of mitigation strategies in the following steps.[93]

*Example 2 (Germany) – Vulnerability Assessment CYTEX 200x (CYTEX)**

Initiated by the *German Group on Infrastructure Protection* (AKSIS),[94] the cyber-terror exercise "CYTEX 2001" was organized in 2001 to study the impact of terrorist cyber-attacks against the CI of an urban region. Participants in this exercise included governmental agencies, major infrastructure providers (such as public services, power generation, telecommunication, public

92 The twelve "Broad Risk Areas" are: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations (Human Resources and Training), and Flexibility/Adaptability.

93 KPMG / National Support Staff. *Predict Defence Infrastructure Core Requirements Tool: Methodology.* http://www.defence.gov.au/predict/general/methodology_fs.htm.

* This section is based on information provided by Thomas Beer, IABG.

94 http://www.aksis.de.

transport, air traffic control, and banks), companies dependent on the CI, and private service providers.

The storyboard entailed coordinated and concerted cyber-attacks of various kinds against CI conducted by a terrorist movement specialized on cyber-attacks. In the scenario, the series of cyber-attacks led to the breakdown of public life for hours, until the functions of the attacked CI could be reactivated as the result of disaster management. The exercise simulated a time period of 24 hours.

The overall aim of the exercise was to study the impact of specific attacks on selected infrastructures in public life, the disaster management process (including the information and communication flow between the actors), steps taken to reestablish the functioning of urban life, and the sensitization of stakeholders.

Various computer simulation models were used in the preparation of the exercise and during the exercise, as a way for the Directing Staff to exercise control. The *Powersim* and *GAMMA* tools were applied. The exercise led to important insights into the vulnerability of infrastructures, disaster management deficiencies, and structural shortfalls.[95]

Example 3 (Netherlands) – KWINT Vulnerability Assessment (KWINT)

♦ The KWINT approach also appears in *Chapter 1: Sector Analysis.*

In 2001, the *Stratix Consulting Group/ TNO FEL* completed the so-called *KWINT-Report* (from the Dutch working title "Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid").[96] The aim of the KWINT report was to analyze the current vulnerabilities of the Dutch section of the Internet,[97] to identify possible consequences of threats, and to determine appropriate measures to reduce the vulnerabilities.[98] The vulnerability analysis was conducted for the social level, the functional level, the structural level, and the physical level (→see Chapter 1 on *Sector Analysis*), as well

95 This section is based on information provided by Thomas Beer, IABG.

96 Luiijf, Eric, M. Klaver, and J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet* (The Hague, 2001). http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf (KWINT Paper).

97 'Internet' was defined end-to-end in this study, to include workstations, private and public IP networks, and information systems on servers.

98 Luiijf, Klaver, Huizenga. The Vulnerable Internet.

as for two additional layers (interaction layer for infrastructures; physical environment). For each of the six layers, the weaknesses, the threat probability, and the possible impact were evaluated using three →*Values (*"high", "medium", and "low"). The vulnerabilities were investigated with respect to four →*IT-Security Objectives*, and with respect to natural causes, deliberate attacks by insiders, and deliberate attacks by outsiders.

This resulted in six tables (matrices) that were aggregated and condensed. The final outcome is a matrix showing the most important vulnerabilities of the (Netherlands' section of the) Internet (Figure 26, excerpt of the whole matrix):

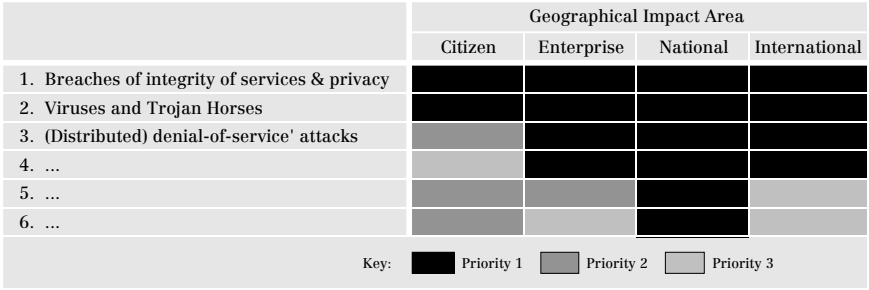

Figure 26: Geographical Impact Area Matrix (Excerpt)

The impacts of selected vulnerabilities on citizens, enterprises, the nation, and society were assessed in this matrix, as were vulnerabilities with global impact (geographical impact area). A number of measures derived from these results were subsequently proposed to the Dutch government.

Example 4 (United States) – DoE Vulnerability Assessment Methodology (DoE)

The *National Strategy for Homeland Security* (2002) and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* clarify federal responsibilities and assign primary responsibility for coordinating protection activities within the energy sector to the Department of Energy (DoE). It is the Office of Energy Assurance (OEA) that leads the federal government's effort to ensure a robust, secure, and reliable energy infrastructure in the new threat environment that includes malevolent threats and increasing complexity due to interdependencies.

The OEA has developed a three-step Vulnerability Assessment Process, described in the *Vulnerability and Risk Analysis Program: Overview of*

Assessment Methodology, published on 28 September 2001.[99] The methodology is divided into three basic phases: pre-assessment, assessment, and post-assessment. Each phase consists of a series of elements or tasks, as shown in Figure 27:

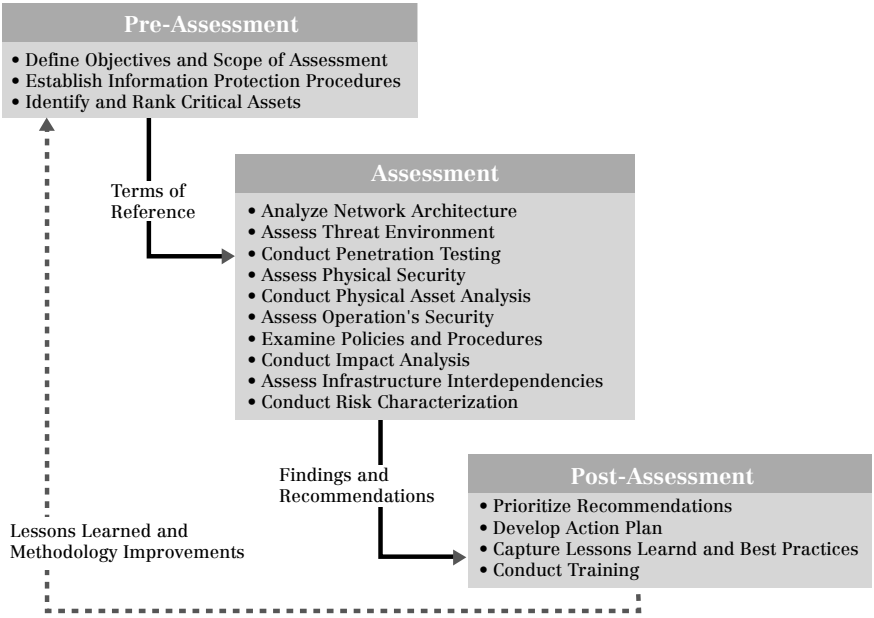

Figure 27: DoE Vulnerability Assessment Process

The updated version of the aforementioned report focuses on the methodology in more detail. Since a general vulnerability assessment methodology is lacking, the DoE has developed a methodology that is tailored to assessing the electric power industry. Companies were asked to consider individually the applicability of the vulnerability assessment elements to their situation.[100]

99 US Department of Energy, Office of Energy Assurance. *Vulnerability Assessment and Survey Program: Overview of Assessment Methodology* (28 September 2001). http://www.esisac.com/publicdocs/assessment_methods/OEA_VA_Methodology.pdf.

100 US Department of Energy, Office of Energy Assurance. *Vulnerability Assessment Methodology. Electric Power Infrastructure* (draft, September 2002). http://www.esisac.com/publicdocs/assessment_methods/VA.pdf.

Example 5 (United States) – CIAO Vulnerability Assessment Process/Project Matrix (CIAO)

On the basis of *Presidential Decision Directive* (PDD) 63 and the National Plan 1.0, CIAO developed "Project Matrix™". It is a program designed to identify and characterize the assets and associated infrastructure dependencies and interdependencies that the US government requires to fulfill its most critical responsibilities. Project Matrix™ involves a three-step process in which each civilian federal department and agency identifies (1) its critical assets; (2) other federal government assets, systems, and networks on which those critical assets depend to operate; and (3) all associated dependencies on privately owned and operated critical infrastructure elements.[101]

The comprehensive methodology as such is confidential. However, a comparable approach, called *Vulnerability Assessment Framework* (VAF), is publicly available.[102] Figure 28 shows the three steps of the VAF Evaluation Process approach.

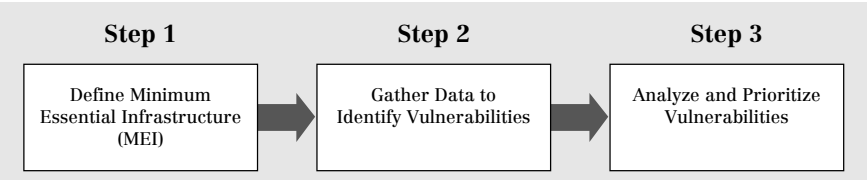

Figure 28: Steps of the VAF Evaluation Process

101 Critical Infrastructure Assurance Office, Project Matrix: http://www.ciao.gov/federal/.

102 KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office* (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf. The VAF methodology draws heavily on other processes for measuring information technology (IT) system controls, such as: the Control Objectives for Information Technology (COBIT) process of the Information Systems Audit and Control Foundation (ISACF); the May 1998 publication "Executive Guide Information Security Management" of the US General Accounting Office (GAO); and the GAO's standards for auditing federal information systems (Federal Information Systems Control Audit Manual, FISCAM).

Step 1: Define Minimum Essential Infrastructure (MEI)

In Step 1, the assessment team defines the so-called "Minimum Essential Infrastructure" (MEI) for the organization. The focus is on the specific infrastructure components that support essential processes. It is recommended that the first step consist of a broad, department- or agency-level macro-vulnerability assessment of both the agency's internal MEI and the agency's relationship to, and connection with, the national MEI.

Step 2: Gather Data to Identify Vulnerabilities

The objective of Step 2 is to identify the vulnerabilities in the organization related specifically to the MEI. The outcome will be the identification and reporting of flaws or omissions in controls that may affect the integrity, confidentiality, accountability, and/or availability of resources essential for achieving the organization's core mission(s). The criteria used to identify these vulnerabilities are depicted in Figure 29, showing the so-called "VAF Cube":

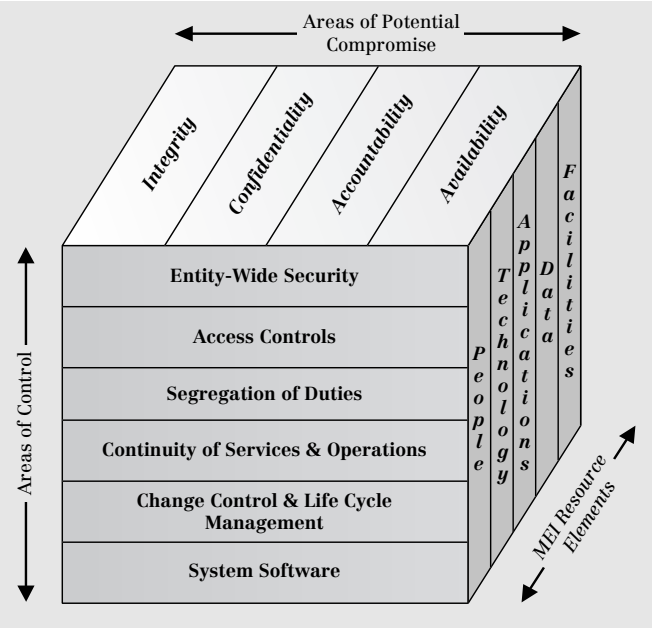

Figure 29: The VAF Cube

Step 3: Analyze and Prioritize Vulnerabilities

In Step 3 the vulnerabilities identified with Step 2 are defined and analyzed. This allows a first order of prioritization for the purpose of remediation or minimization. Figure 30 shows the activities conducted in Step 3:

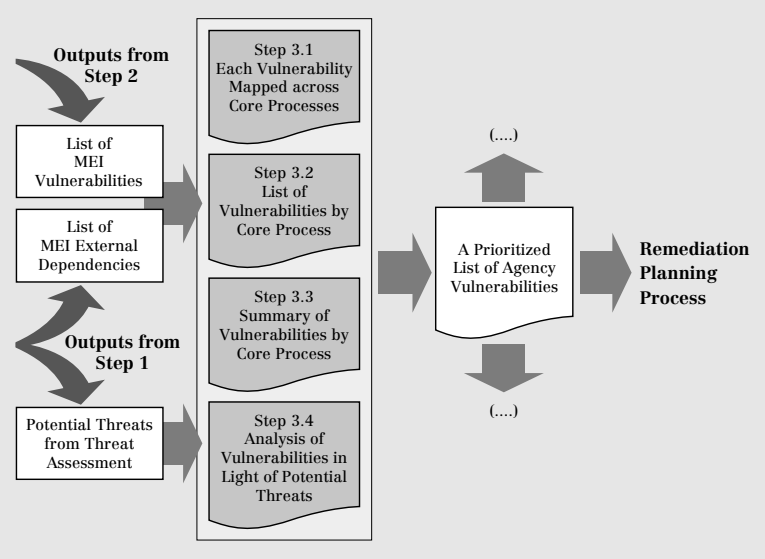

Figure 30: Step 3 Activities

Step 3 includes four sub-steps: (1) Each vulnerability is examined to determine if it has an impact on more than one MEI core process; (2) vulnerabilities are sorted by core processes; (3) a graphical summary of the number of vulnerabilities by core processes is generated; (4) an analysis of the likelihood that a vulnerability will be exploited is conducted, taking into consideration the potential threats to the agency. Using these four parameters, priorities are assigned for vulnerability remediation or minimization.