4 Threat Assessment

As critical infrastructures deliver a range of services that individuals, and society as a whole, depend on, critical infrastructures are a favored target for malicious attacks. Any damage to or interruption of critical infrastructures causes ripples across the technical and the societal systems – this principle held true in the past, and even more so today due to much greater interdependencies. Attacking infrastructure, therefore, has a "force multiplier" effect, allowing even a relatively small attack to achieve a much greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors.[72]

The US Presidential Commission on Critical Infrastructure Protection (PCCIP), for example, defines "threat" as a "foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security. A threat may be an individual, an organization, or a nation."[73] In publications on security of IT systems, threats are seen as the potential for a particular threat-source to successfully exploit a particular vulnerability, which means that a threat-source does not present a risk when there is no vulnerability that can be exercised.[74] Threats do not necessarily need to originate from human sources, but can be natural, human, or environmental.

What is Threat Assessment?

On the side of the government, the ability to gauge threats to critical infrastructure has traditionally depended on the ability to evaluate the intent of an actor, coupled with the motivation and the capability to carry out the action. This was easier when dealing purely with securing the physical realm – the nature and magnitude of physical threats have evolved relatively slowly over time, allowing for the establishment of indicator and warning mechanisms

[72] Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Threat Analysis* no. TA03-001, 12 March 2003. http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf, p. 34.

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

[74] 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. 12.

– but it was different for the rapidly evolving and little-known cyber-threats.[75] However, with the advent of cyber-based threat actors, the “enemy” becomes a faceless and remote entity, a great unknown almost impossible to track, opposing security institutions and laws that are ill suited to counter or retaliate against such a threat, while the overall capability of such malicious actors to do harm is believed to be enhanced by inexpensive, ever more sophisticated, rapidly proliferating, easy to use tools in the cyber domain.

Threat assessment in the risk analysis sense includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, it should be kept in mind that terrorism is an actor-based threat that is intrinsically non-quantifiable.[76]

Examples of Threat Assessment Aspects

In the following sections three different aspects of threat assessment are described: a management methodology, a general description of the threat environment, and an IT risk analysis approach.

- Example 1 (Australia) – NSW Risk Management Methodology (NSW)
- Example 2 (Canada) – OCIPEP Paper on Threat Analysis (OCIPEP)
- Example 3 (United States) – NIST Risk Management Guide (NIST)

Example 1 (Australia) – NSW Risk Management Methodology (NSW)

The example of the NSW risk management methodology shows that looking at CIP/CIIP from the point of view of threat can substantially impact on the way the infrastructures are assessed: When the list of critical infrastructures was validated with all stakeholders – this was achieved in five managed sector-specific workshops that included all owner/operators and policy owners from the utilities, transport, emergency services, major hazards (chemical), and medical sectors – it became necessary to evolve beyond the conventional ‘sector’-based focus. The threat assessment was based on an *Australian Security Intelligence Organisation (ASIO) Context Statement*

[75] OCIPEP, *Threat Analysis*, p. 12.

[76] 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 (Center for Security Studies, Zurich, 2003), p. 61.

concerned with terrorist threat.[77] During the workshop, participants became aware that terrorists might attack not a whole sector, but rather key elements of an infrastructure.

Hence, it became clear that the notion of an attack on an infrastructure or a sector as a whole is not particularly useful. Categorizing targets in terms of their inherent function (such as raw material supply, distribution node, or command and control center) was considered far more meaningful. The notion of a more manageable 'target category' evolved in this context. This approach also facilitated a far better understanding of the differences between the sectors in terms of their perceptions of 'consequence' and 'vulnerability'. For example, the time at which an outage has an adverse effect on the population and the environment varies dramatically from sector to sector. This had to be taken into account to ensure the accuracy of the final risk assessment.[78]

The *NSW Information Security Guideline Part 2* on threats and vulnerabilities provides examples of the threats posed to information assets. It also identifies the vulnerabilities to be considered in the process of risk assessment. The guideline addresses the following key areas:

- The general definition of threats and vulnerabilities in relation to information assets;
- Environmental threats resulting in the loss of availability of information, such as natural disasters, contamination, and power fluctuations;
- Accidental threats arising from human errors and omissions, including fire, communication failures, and technical difficulties;
- A threat, whether it comes from an internal or external source, has the potential to cause harm to information assets, in which it exploits vulnerabilities. Vulnerability can be a weakness in the physical environment, organization and management, procedures, personnel, operations, software and hardware, or communications equipment.[79]

[77] http://www.asio.gov.au/.

[78] Yates, Athol. *Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment* (Institution of Engineers, Australia, June 2003). http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf, p. 65.

[79] New South Wales Office of Information and Communications Technology's (OICT), *Information Security Guideline for NSW Government Part 2 – Examples of Threats and Vulnerabilities*, No. 2.0. First published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.17-Security-Pt2.htm.

Example 2 (Canada) – OCIPEP Paper on Threat Analysis (OCIPEP)

A paper published by the Canadian *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP) in March 2003 aims to provide a taxonomy of the threats seen as most likely to impact upon Canada's national critical infrastructure.[80] The report, which does not focus exclusively on the cyber-infrastructure, wants to provide owners and operators, emergency managers, and the government with baseline information regarding potential threats to the networks and systems.

The publication defines the threat environment by the interaction of the infrastructure elements and the threat agents (Table 4). The means of attack or incident can be both physical and cyber-based. The target can be virtual, such as the information or applications on a network, or physical, such as a telecommunications cable. In reality, it is becoming increasingly difficult to distinguish between purely physical and cyber components of the infrastructure:

		Means	
		Physical-based	*Cyber*-based
Target	*Physical*	-Bombing of hydro tower - Severing a telecommunications cable with a backhoe - Explosion at an oil refinery - Ice storm debilitating hydro towers	- Hacking into the SCADA system that controls municipal sewage and water - Geomagnetic storms affecting CI elements
	Virtual	- Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components.	- Hacking into a critical government network - Penetrating the SS7 telecommunications transmission controls

Table 4: The CI Threat Environment[81]

The publication distinguishes between natural, accidental (physical and cyber), and malicious threats (physical and cyber) against CI and CII. In the context of CIIP, the characteristics of malicious computer-based threats to CI/CII ("cyber-based means"), which make them both difficult to predict and detect, are especially interesting:

- The problem of actor identification is particularly difficult in a domain where maintaining anonymity is easy and where there are sometimes time lapses between the intruder action, the intrusion

[80] Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), *Threat Analysis* no. TA03-001, 12 March 2003. http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.

[81] Ibid., p. 12.

itself, and the actual effects. In addition, the continuing proliferation of sophisticated computer technologies into the mainstream population makes assigning attribution increasingly difficult.

- The threat is not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world, and may be launched from multiple locations simultaneously. Investigations and backtracking through a web of false leads and unwittingly slaved systems can be time-consuming and resource-intensive.
- The threat environment is extremely fluid. The window of opportunity between the discovery of vulnerabilities and the elaboration and implementation of a new tool or technique to exploit the vulnerability is narrowing rapidly.
- Technologies for attacks are simple to use, inexpensive, and widely available. Computer intruder tools and techniques, for example, are widely available on computer bulletin boards and various websites, as are encryption and anonymity tools.
- The methods of attack have become increasingly automated and more sophisticated, resulting in more damage from a single attack.
- The methods and tools used for attacks are often similar or identical to technologies used to ensure network reliability.
- The cost required to develop a significant attack capability continues to decrease.

Example 3 (United States) – NIST Risk Management Guide (NIST)

The *Risk Management Guide for Information Technology Systems* of the National Institute of Standards and Technology (NIST) sees threat assessment as a step in the overall risk analysis process. The aim is to identify the potential →*Threat-Sources* and to compile a list of threats applicable to the IT system. A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat-sources for the CII can be natural, human, or environmental:[82]

- *Natural Threats*: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- *Human Threats*: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry)

[82] 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. 13.

or deliberate actions (network-based attacks, malicious software upload, unauthorized access to confidential information).

- *Environmental Threats*: Long-term power failure, pollution, chemicals, liquid leakage.

The *Risk Management Guide* states that it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. Humans may be threat-sources through intentional acts (such

Human Threat-Sources	**Motivations**	**Methods/Threat Actions**
Hacker, cracker	Challenge, ego, rebellion	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer crime (e.g. cyber-stalking) Fraudulent act Information bribery Spoofing System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	Assault on employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access

Table 5: Human Threats – Threat Source, Motivation, and Threat Actions[83]

[83] Ibid., p. 14.

as deliberate attacks by malicious persons) or unintentional acts (such as negligence and errors). A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality, or (2) a benign, but nonetheless purposeful, attempt to circumvent system security.

Individuals with the motivation and the resources for carrying out an attack are potentially dangerous threat-sources. Table 5 shows an overview of common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack, as identified by the Risk Management Guide. This information is considered useful to organizations studying their human threat environments and customizing their human threat statements.

After the identification of the potential threat-sources an analysis of the possible motivation, resources, and capabilities should be undertaken in order to determine the likelihood of a threat exercising a specific vulnerability[84] (→see also Chapter 3 on *Risk Analysis*).

[84] Ibid.