Multinational Experiment 7

Outcome 3 – Cyber Domain

Objective 3.1

Threats and Vulnernability Methodology

Version 1.0

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Multinational Experiment 7 Outcome 3 ¨C Cyber Domain Objective 3.1 Threats and Vulnernability Methodology Version 1.0	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
This document presents a generic methodology designed to support decision©makers in enhancing resilience through a better understanding of how their nation or organization is dependent on the cyber domain, and how they can be better prepared to maintain essential capabilities and services in the event of cyber attacks on their critical assets. The main body of the concept is a step© y©step guide to the practical application of the methodology. It takes a working group through the identification of an organization¡¯s critical assets, analysis of its dependencies on cyber space and any associated vulnerabilities, and the need to maintain a current threat picture. Finally it introduces mitigating measures that will help make a system more resilient. As this methodology is designed to be generic, some parts of it will be more relevant than others for your organization and your specific level within that organization. While the methodology is presented as a whole, parts of it can also be standalone or used as separate methods as appropriate.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**39**	

Executive Summary

Societies are becoming increasingly dependent on the cyber domain, a man-made domain where developments continue to take place at an extremely rapid pace. Historically, in the traditional battle domains, attacks on critical assets could be deterred through the display of overwhelming offensive capabilities. With the introduction of cyberspace, this is no longer the case. Often, one will not be aware of a threat until an attack has taken place, and even then it will be arduous to prove its point of origination. When traditional deterrence is no longer an option, other preventive or protective measures must be considered. This concept promotes resilience: accepting the risk that an attack will take place, and focusing on improving the ability to prevent, detect, absorb and recover from it. There are in fact universal mitigating measures with "guaranteed effect" that make systems more resilient to cyber attacks.

This document presents a generic methodology designed to support decision-makers in enhancing resilience through a better understanding of how their nation or organization is dependent on the cyber domain, and how they can be better prepared to maintain essential capabilities and services in the event of cyber attacks on their critical assets. The main body of the concept is a step-by-step guide to the practical application of the methodology. It takes a working group through the identification of an organization's critical assets, analysis of its dependencies on cyber space and any associated vulnerabilities, and the need to maintain a current threat picture. Finally it introduces mitigating measures that will help make a system more resilient. As this methodology is designed to be generic, some parts of it will be more relevant than others for your organization and your specific level within that organization. While the methodology is presented as a whole, parts of it can also be standalone or used as separate methods as appropriate.

For those interested in understanding the conceptual basis upon which the methodology rests, Annex A explains the theoretical principles and key definitions. Annex B contains "Ten Commandments of Resilience" - an 'aide memoire' for achieving resilience, while Annex C contains a "Methodology Crosswalk" – a handy two-page form which will aid you in finding the right section in the methodology for the particular task with which you are dealing, as well as identifying potential outputs for each step.

Table of Contents

1.0 Methodology for Enhancing Resilience

This step-by-step methodology aims to support decision-makers in gaining a better understanding of how their nation or organization is dependent on the cyber domain, and of the types of cyber-related threats and vulnerabilities that pose a risk to their critical assets and functions. This methodology will guide a working group through the steps necessary to improve the cyber resilience of its organization: Analyzing critical functions and infrastructure; discovering their dependencies on cyberspace; revealing their vulnerabilities; conducting dynamic threat analysis; and finally, increasing resilience through mitigating mechanisms.[1]

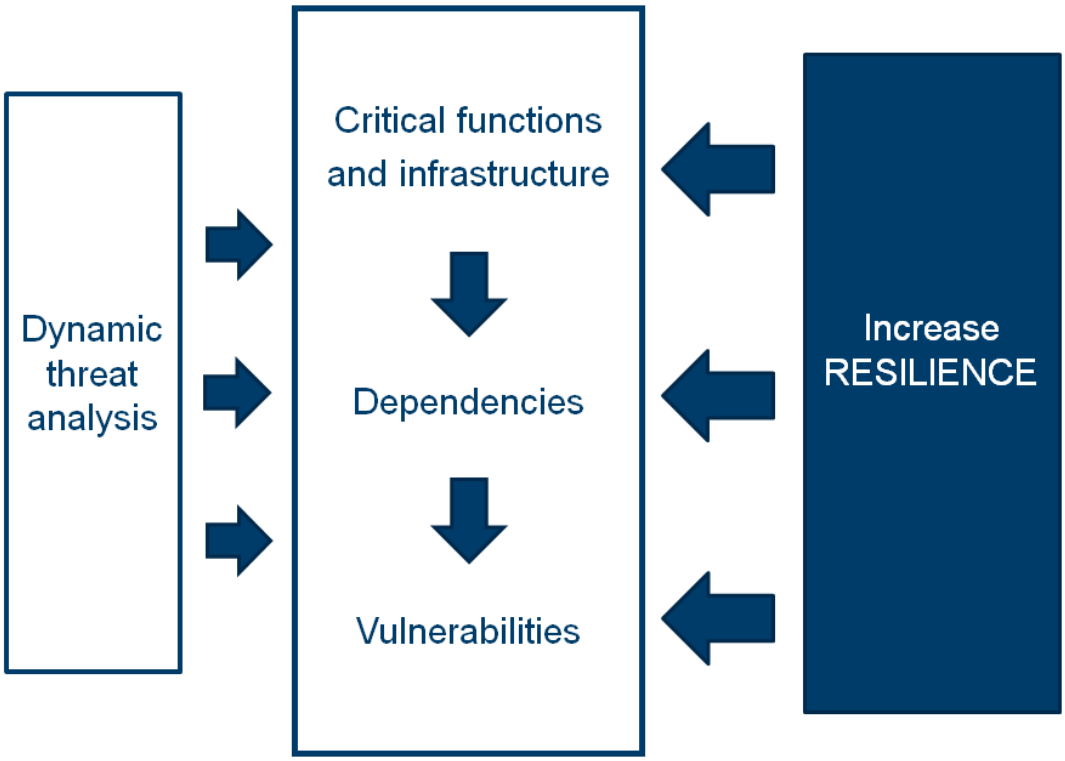


Figure 1. Methodology for enhancing resilience

In order for such a working group to be able to fulfill this mandate, it must have as complete an understanding of the organization as possible. To achieve this, the composition of the group is critical. Representatives from the organization's management at a sufficiently high level (on the

[1] Keep in mind that different organizations of varying sizes will have very different resource levels: scope your efforts by determining which assets are most critical, which vulnerabilities are most serious, and which threats are most dangerous in order to prioritize.

national level the executive office) need to be included, as well as technical experts. The level of the participants must match the mandate, and they require sufficient security clearances to access the information needed. At the national level it is suggested that the working group should include, but not be limited to, representatives from the following sectors: communications, emergency services, energy, finance, food, government and public services (including defense), health, transport, and water.[2]

Applying traditional risk analysis to the cyber domain has proved challenging, due to the need for as reliable data as possible on a large number of variables in order to provide accurate risk estimates. Whilst some data can be obtained for known threats (based on attacks that have already happened elsewhere) the rapid pace with which developments occur in the cyber domain means there is insufficient data on potential future threats. Hence the focus on resilience; an understanding of the dependence of our own critical systems on cyberspace, the inherent vulnerabilities this creates, and ensuring that alternative means of providing necessary capabilities and services are in place. The degree of resilience in a system represents its ability to maintain the capabilities or services provided by the attacked asset through the mechanisms of prevention, detection, absorption and recovery during and after an attack. Prevention is about reducing dependencies and vulnerabilities before an attack has been launched; detection is about detecting and dealing with an attack in the most effective manner as it occurs; absorption is about reducing damages during an attack; while recovery is about rapidly returning to a stable condition after an attack has been carried out.[3]

A set of universal mitigating mechanisms to enhance resilience have been identified:[4]

- Building awareness
- Reducing dependencies
- Increasing redundancy
- Developing alternative back-up solutions
- Increasing adaptability
- Transferring risk
- Sharing information[5]

[2] Moteff, John, Claudia Copeland, and John Fischer (2003);
Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke (2011)
[3] See Annex A for detailed discussion of both traditional risk analysis and resilience.
[4] See Annex A (*VIII. Resilience: an alternative to deterrence*) for further information on what these mechanisms entail.
[5] Multinational Experiment 7 – Objective 3.2 Concept (2012). "*Information Sharing Framework*".

2.0 Prevention

Prevention can include both active and passive measures. Active prevention can be interdiction or elimination of known threats before an attack occurs, requiring detailed knowledge about specific threats, however, as this takes the discussion beyond the purely defensive, it will not be considered further in this methodology. This methodology will focus on passive prevention measures resulting in more resilient systems.[6]

2.1 Identifying critical assets

The first step is to identify the national or organizational key, or critical, assets. This process is referred to as a criticality analysis, and can be simply addressed through the question "How essential is this asset to your mission?"[7]

Table 1 provides a guide to assessing the criticality of assets and/or processes:

CRITERIA	**QUESTIONS**
Impact on life and health	If the process is disrupted, what is the impact on human life and health?
Time frame	If the process is disrupted, how long will it take to have an impact on the organization's overall product/service? Generally speaking, the shorter the time before a disruption has impact, the more critical the process is.
Magnitude	How much of the overall product/service will be affected if this process is interrupted or completely stopped?
Contractual, regulatory, or legal relevance	If the process is disrupted, what contractual, regulatory or legal consequences will this have for the organization?
Economic damage	If the process is disrupted, what is the estimated financial damage to the organization?
Social damage	If the organization fails to deliver the products/services to which it has committed, what could be the social damage? For example, how will such a disruption damage the public confidence in the organization?

Table 1. Criticality Criteria

The working group should decide which criteria to use, how many criteria should apply at once and which classifications to use within the criteria, depending on their knowledge of the organization. Identifying key assets is perhaps the least challenging task for the working group,

[6] See Annex A for a more detailed discussion of the concept of resilience, and why it is difficult to use more offensive prevention measures when dealing with the cyber domain.
[7] Brown, Gerald, Matthew Carlyle, Javier Salmerón, and Kevin Wood (2006)

as the organization itself possesses all of the necessary information, however for large organizations it can prove to be highly complex.[8] This is also the step in which it becomes essential that the members of the working group have the necessary clearances to fulfill its mandate.

The criticality analysis will result in identification of all critical processes in an organization and portraying their sub-processes as well as their "risk elements". Risk elements can include people, facilities and equipment, data and files, grounds and buildings, as well as other resources. Most nations and organizations will have to accept that resource limitations will mean that not all assets can be equally secure and that a prioritization of efforts is necessary. A degree of prioritization can be achieved by identifying those components on which a number of critical infrastructures and services are dependent. In addition it may become apparent that there are critical dependencies that lie outside the control of the organization or nation[9].

2.2 Dependency analysis[10]

Once the working group has determined the mission critical functions, assets and processes in the nation or organization, it should then assess their dependence on the cyber domain. Any cyber dependency is a potential vulnerability. In order to determine specific cyber dependencies there needs to be a clear understanding of the underpinning functions, assets, and processes at the levels below that at which the criticality assessment was carried out.

2.2.1 Analysis of supply chain and value chain: A supply chain approach is a useful tool for exploring dependencies "upstream and downstream" from the organization. A supply chain can be defined as a network of autonomous or semiautonomous entities collectively responsible for an end result, which could be a product, function, or a service. While these entities can operate under different constraints in order to reach different objectives, they are highly interdependent.[11] By considering an organization's assets from a supply chain perspective, one can break a large, unwieldy system into more manageable elements that can be analyzed for dependencies on cyberspace. Such dependencies can be both internal to each element (software and hardware) and external in the form of linkages. One could also consider the problem in the opposite direction from a value chain perspective. The aim is to answer the question "On whom

[8] It could prove useful to enter all of the information into a database, which can later be updated when necessary.
[9] Such dependencies can become the subject of agreements between custodians to secure critical deliveries as a measure of risk reduction.
[10] Multinational Experiment 7 – Objective 3.1 Workshop Input from the United Kingdom (2011a)
[11] Swaminathan, Jayashankar M, Stephen F. Smith, and Norman M. Sadeh (1998)

are we dependent for services and who is dependent upon us?" Having established that, interfaces and touch-points with cyberspace can be identified.[12]

The working group will be responsible for deciding how far, "upstream and downstream," in an organization's chains cyber dependencies can reliably be identified, in order to set the outer boundaries for the exploration. During this process any prioritization will be based on expert knowledge provided by those actively involved in the processes in question. The list of identified dependencies is likely to be extensive, with a significant number lying outside the responsibility of the organization conducting the dependency analysis. However, managing external dependencies is a critical component of resilience and must be addressed by appropriate mitigation measures.

Figure 1 illustrates a petroleum supply process, the dependencies within its supply chain, and how at each point in the chain there are key assets dependent on the cyber domain. Complex processes should initially be considered at high level, as portrayed below, but there will be a requirement to drill down into specific individual processes to reveal further detailed dependencies on cyberspace.[13]

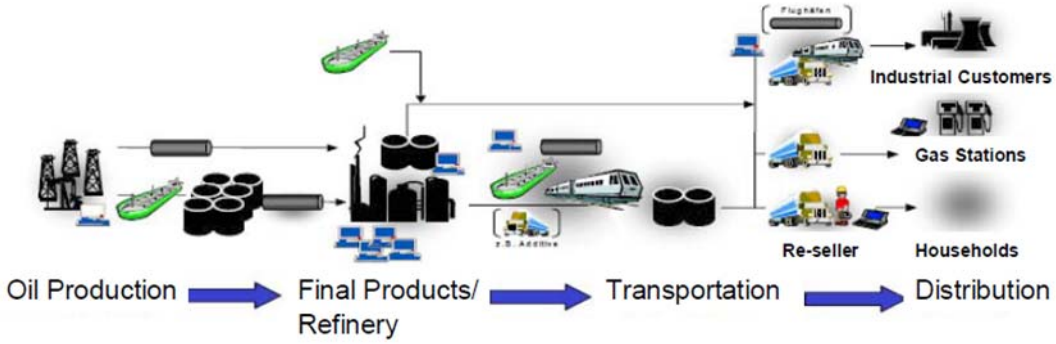


Figure 2. Petroleum Supply Chain

2.2.2 Prioritizing: The criticality analysis will have determined those assets and infrastructures that are deemed critical to the nation or organization. Now a decision has to be made as to which cyber dependencies within those critical assets are critical to the provision of the capability or service, and require additional attention and potentially mitigating action.

[12] Feller, Andrew, Dan Shunk, and Tom Callarman (2006)
[13] This figure is from the Multinational Experiment 7 – Objective 3.1 Workshop Input from Germany (2011):11

This can be done by asking these key questions:[14]

- Is a particular dependency critical to the provision of more than one capability or service?
- Is it possible to use redundant or alternative back-up systems to perform this specific function?
- How complex and time-consuming would it be to switch to redundant or alternative back-up systems?
- If there is no redundancy or alternative back-up system, for how long can the organization go on without the specific function?
- How complex and time-consuming would it be to put the function back into order?[15]

If it is discovered that there are cyber dependent functions not supported by redundant or alternative systems, and the organization can only go for a very short time, if at all, without it, the working group should consider mitigating action as a matter of urgency.

2.2.3 Mitigating action: Although mitigation can be considered at this stage, an understanding of the risk posed by a dependency will be better understood after the vulnerability analysis. An initial determination of which dependencies could require mitigating action, and which efforts can be made to reduce the cyber dependencies discovered, may be made at this point. However, ultimately a cost-benefit analysis will be required to justify any mitigation.[16]

2.3 Vulnerability analysis[17]

A threat needs one or more vulnerabilities to materialize itself in a system. The next step is therefore to perform an analysis of the dependencies to identify the potential vulnerabilities in the system or organization. To perform such an analysis in practice, it is useful to go through four steps: Identification, Impact Analysis, Assessment, and finally Mitigation.

[14] Multinational Experiment 7 – Objective 3.1 Workshop Input from the United Kingdom (2011a)
[15] Multinational Experiment 7 – Objective 3.1 Workshop Input from the United Kingdom (2011a)
[16] See Annex A (*VIII. Resilience: an alternative to deterrence*) for further information on these mechanisms; Whilst discussing protection against future events there is an assumption that the organization is compliant with current "best practice" regarding cyberspace, such as adoption of the latest patches for known problems, current software versions and training of personnel.
[17] The overarching theme of this section is from the Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b).

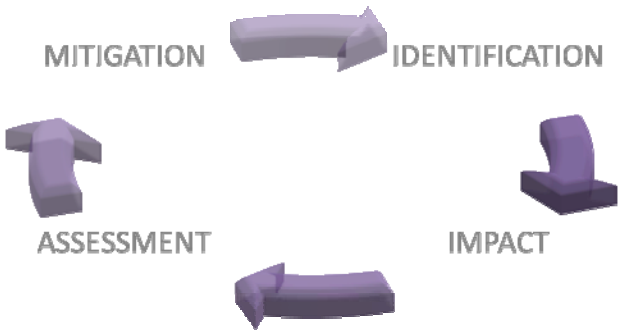


Figure 3. Vulnerability Analysis

2.3.1 Vulnerability identification:[18]

To identify vulnerabilities it is essential to look at the system as a whole, and bring together the cyber dependencies identified above with the relevant risk elements. Risk elements include people, facilities and equipment, data and files, grounds and buildings, as well as any other resources. It is useful to divide the cyber domain into four layers, each with its unique potential to generate vulnerabilities: users, applications, fundamental services, and communications infrastructure.

CYBER DOMAIN	Users	Vulnerabilities of a logical, social or physical nature
	Applications	
	Fundamental Services	
	Communications Infrastructure	

Table 2. Layers of the Cyber Domain

Users are often operators of command and control systems within critical infrastructures, and can in some ways be considered critical assets themselves. The application layer makes up the command and control system for the critical infrastructure. That includes operating systems and applications for users and the servers, server software, and databases. The two lower levels are fundamental services; and the communications infrastructure, consisting of transmission systems, transport and access networks. Any vulnerability in these areas could potentially affect many systems. [19]

[18] Fridheim, Håvard and Janne Hagen (2007);
BAS 5-prosjektet (2007)
[19] Fridheim, Håvard and Janne Hagen (2007);
BAS 5-prosjektet (2007)

A list of vulnerability classes is given below and should be examined against each of the four layers of the cyber domain. The structure of the list reflects the four layers: the first issues are mostly relevant to the higher layers, while the classes further down the list are more relevant to the lower layers. There is also overlap between the higher and lower levels.

Vulnerability classes: [20]

- **Security program:** Roles and responsibilities for security, human and financial resources, security policies and procedures
- **Sharing of Information and Assets:** Policies and procedures for sharing
- **Geographical location:** Different security environments exist within and outside of your own country
- **Contracting:** Security requirements and facility security
- **Security Awareness:** Level of security awareness and training in the organization
- **Access limitations:** Limitations on access to critical assets
- **Security Screening:** Security clearances and site access procedures
- **Physical Security:** Perimeter security, facility management, secure storage and transport
- **Information Technology Security:** Technical measures, out of date technology etc.

2.3.2 Vulnerability impact analysis:[21]

Once the vulnerabilities have been identified, the working group should analyze the possible consequences of exploitation.

The group can analyze the impact on the organization based on the variables in Table 1, repeated below:

- Impact on life and health
- Time frame
- Magnitude
- Contractual, regulatory, or legal relevance
- Economic damage
- Social damage

[20] These classes are based on the Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b):7-9

[21] Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b)

2.3.3 Vulnerability assessment:[22]

The working group must assess whether the impact analyzed is characterized as serious enough to warrant mitigation (some mitigation mechanisms are relatively cheap and quick, such as some forms of training, while others are more costly). It should be noted that vulnerabilities are not solely 'inadequacies' in a system, as the attribute representing a vulnerability could be among the most positive attributes of an asset.[23]

The working group can use the figure below as a tool in assessing the criticality of an identified vulnerability. It can be assessed qualitatively in relation to the organization as a whole, or to specific critical functions or services. Note that the figure is a simplified illustration, as the variables in reality will be more dynamic and will vary in time.

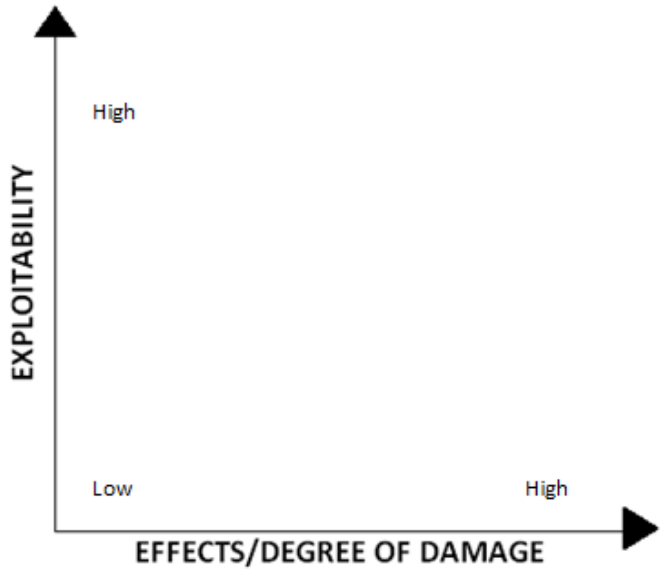


Figure 4. Vulnerability Assessment

Exploitability is a qualitative measure for how 'easy' it would be to exploit a specific vulnerability. Variables include the knowledge necessary for exploitation, how accessible the vulnerability is, etc.

Effects/Degree of Damage (impact) is a qualitative measure for the effect or damage an exploited vulnerability could have for the organization at large, or for critical functions.

[22] Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b)
[23] One example is a laptop computer: while its portability is among its most positive attributes, it is also an attribute which makes the asset vulnerable, as it can be stolen or otherwise compromised more easily than a stationary computer set inside of an office building (Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b)).

Vulnerability mitigation

What should be done to counter the vulnerabilities that have been analyzed? This is where universal mitigating mechanisms (defined in Annex A) should be considered, and where they can be transformed from being more abstract concepts into actual policies:

- Building awareness
- Reducing dependencies
- Increasing redundancy
- Developing alternative back-up solutions
- Increasing adaptability
- Transferring risk
- Sharing information

2.4 Threat analysis[24]

In parallel with examining the organization's key assets, dependencies, and vulnerabilities, the working group should update and maintain an understanding of the threats facing it. The extent of threat analysis an organization can feasibly conduct depends on the size and type of organization. States, government agencies, and large corporations will be able to focus on these issues in a much more detailed manner than can small companies. Looking at previous attacks, analyzing the trends, one can hope to identify previous threatening actors. Whilst situational awareness of cyberspace can provide an understanding of what has happened, it is almost impossible to predict the nature of a future threat – hence the need to address resilience.[25]

Being a relatively new and rapidly developing domain, cyberspace is perhaps particularly prone to Black Swan events: events that are a surprise (to the observer), have a major impact, and are after the fact rationalized with the benefit of hindsight. A threat analysis will be very specific to a nation or organization, based on a range of different factors (purpose, political alignment, threat actor capabilities etc.) and to a significant degree based on its understanding of the environment and ability to detect changes within it – local situational awareness from all domains. This can

[24] The structure of this section is based on the Multinational Experiment 7 – Objective 3.1 Workshop Input from Spain (2012);
Note that intentional attacks are not the only catalysts of major incidents – hazards such as natural catastrophes, lightning strikes, dams breaking, etc. could also be potential causes of disruption.
[25] Multinational Experiment 7 – Objective 3.2 Concept (2012). "*Information Sharing Framework*".

be further enhanced by drawing on information from further afield – thereby gaining earlier warning of potential threats.[26]

In addition, an understanding of which types of threats are of particular relevance may be further assisted by dividing them into categories. Common categories include:[27]

- Criminal Groups
- Hackers
- Hacktivists
- Insiders
- National Governments and Foreign Intelligence Services
- Terrorist Groups[28]

Once the categories most relevant to the organization have been identified, the potential rationale for attacking the organization might become evident. A proposed general classification, together with threat actors, is given here:[29]

- Economic benefits: Computer criminal, industrial spy and insiders
- Tactical/Competitive advantage: Insiders, industrial spy and nations
- Political: Terrorists and hacktivists
- Destruction/Damage: Terrorists
- Fame or vengeance: Hackers

Keep in mind that these categories are dynamic, and that the same actor can move across the spectrum of both organization and rationale at their own discretion.

A threat assessment draws on information from all domains to generate context. Some threats are calendar-driven, and can therefore be predicted with some certainty, while others are a direct result of an unpredictable event, or response to an event, over which one has no control. An example of the former is increased risk of hacktivism surrounding controversial political events or acts (such as elections that are perceived as less than free and fair), and an example of

[26] Andress, Jason and Steve Winterfeld (2001):257
[27] Multinational Experiment 7 – Objective 3.1 Workshop Input from Spain (2012);
Note that this list is not all-encompassing and complete, but is a very useful general starting point.
[28] In the event of what is usually thought of as a terrorist attack it is more likely that cyber means will be part of a combination attack along with more physical/traditional attack vectors, rather than cyberspace being the only means used.
[29] Multinational Experiment 7 – Objective 3.1 Workshop Input from Spain (2012);
Different types of malignant actors act in different ways: spies and thieves have different end goals, and will therefore have different modus operandi. Knowing which kind of threat actor you are facing will help you put the right types of defensive mechanisms into place.

the latter is Danish companies being targeted by groupings insulted by the Muhammed caricatures.

Once the most relevant threat actors and their motivations have been established, the answers to the following questions can be refined:[30]

- Out of the people or groups posing a threat to the organization, who has information and capacity to threaten our key functions?
- What are their goals? What are these groups trying to achieve?
- What is known about their strategies? How do they usually operate?
- What do they already know about the organization that can be used against it?
- What can be done to mitigate these threats?

3.0 Detection

The effectiveness of any detection mechanism is a measure of two attributes: the degree of certainty that it will expose certain threat events, and the efficiency with which it operates to prompt an early response. The working group should therefore examine the organization's policies in place for dealing with detected cyber events[31], incidents[32], and attacks.[33]

The most important part of the detection process is to find out *what exactly has happened*. This includes defining the attack by asking "What is being attacked, and how?", as well as categorizing the attack by asking "What type of attack is this, and which vectors are used?" In support of this, one can use the process known as Triage, ranking the events, incidents and attacks in terms of importance or priority. This will normally start with categorization against a list for which pre-defined responsibilities and actions have been derived. [34] This process continues into the Absorption and Recovery phases.

Another important question for the working group to ask, is: "What is the average (or estimated) length of time between an attack and when it is discovered?" If this takes a long time, the working group should consult with technical experts in order to improve. Without clearly

[30] These questions are based on a set of OPSEC questions from Holm, Ola (2004):25
[31] An event is a single observation that may or may not have any significance.
[32] An incident is a collection of events that are regarded as linked and need to be investigated.
[33] Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011a)
[34] ISO/IEC 27035 – Generic incident types include Malware, Network Attacks, Information Destroy, Content Security, Facilities Faults, Disaster, Loss, Theft, Disclosure, Fraud, Hoax, Communications, Physical, Procedural, and Others.

established readiness levels and associated security procedures, the response to incidents may be too slow or incomplete.[35] Generally, the faster the organization acts once it has been attacked, the less damage the attacker can do.

The working group should then go on to ask the following:

- How are incidents reported internally in the organization?
- Who is in charge of this process?
- Do the policies in place ensure that information about the attack is shared internally (for instance to those who will be affected)?
- Which policies are in place for information sharing externally (with government, sector, etc.)?
- What does the organization do if it is alerted of an incident that has occurred elsewhere in the world, but against similar hardware/software to its own?[36]

4.0 Absorption

Absorption is about creating damage-tolerant systems that serve to contain, soak-up or deflect the consequences of an attack – maintaining capabilities and services despite an attack. It also allows decision-makers enough time to analyze the problem before a critical decision must be made on how to respond.

Experts should be consulted, as there are several technical options for managing an attack once it has been detected. An example is the ability to contain a detected attack (for instance a virus) in a specific part of your system, allowing technical experts to observe the attack in a "safe" environment. Observing its behavior in such a way could help improve resilience.

In addition to the technical aspects, for absorption to be effective there needs to be clear policies and guidelines in place as to what should happen next. This can be done by asking the following questions:

- Who is in charge of the different aspects of the absorption process?
- How do we identify which systems and users are affected by this incident?
- Who should be informed that there has been a breach?[37]

[35] Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b)
[36] See Multinational Experiment 7 – Objective 3.2 Concept on Information Sharing (2012) for more on the issue of sharing information about detected cyber attacks.

The organization should also have developed a business continuity plan, in order to continue "business as usual" (or as close to this as possible). Below is a list of suggested aspects that could be included in such a plan:

- Identify the stakeholders in an emergency situation.
- Define roles and responsibilities.
- Set up clear procedures for command and control.
- Identify critical assets, functions, and services.
- Decide maximum allowable downtimes and minimum service levels (Mean time to recovery, the average time taken to put a defective component or system back in working order, could prove a useful measure in this process).
- Identify interdependencies between assets.
- Identify dependencies on cyberspace.
- Identify redundant systems.
- Identify alternative back-up systems.
- Determine how to achieve secure synchronization between primary and secondary systems.
- Ensure alternatives are operating, trained for, and practiced.
- Ensure all "protective" measures are in place and up to date (anti-virus, patches, policies, training, etc.).
- Create a communications strategy for effective public relations.[38]

Once the working group has created its business continuity plan, it should be regularly tested. The test should be followed by an after action report, which should answer these questions:[39]

- What happened?
- What should have happened?
- What went well?
- What went poorly?
- What will we do different in the future?

---

[37] See Multinational Experiment 7 – Objective 3.2 Concept on Information Sharing (2012) for more on the issue of sharing information about cyber attacks.
[38]Wallace, Michael and Lawrence Webber (2010):14-20;
Stanton, Ray (2005);
Gibb, Forbes and Steven Buchanan (2006);
Multinational Experiment 7 – Objective 3.1 Workshop Input from the United Kingdom (2011b)
[39] Wallace, Michael and Lawrence Webber (2010):20

5.0 Recovery

An important part of enhancing resilience is having the ability to recover after a cyber attack. The consequences of an attack can vary greatly depending on the type of attack. Some examples include having to restore a section of critical infrastructure, changing a number of login credentials that have been stolen, or trying to calculate how much it will cost to redesign components of a system that you think the adversary might have compromised. The effectiveness of your response to an attack will be directly proportional to the robustness of your planning ahead of an attack, and any inadequacies related to business continuity planning could delay the resumption of critical services after an unwanted event.

First of all, the working group should decide who in the organization has the authority to give the "all clear" for a system to be reloaded after an attack. Who decides when the system is officially "recovered"? And how is this decided? While one could assume that recovering a system as fast as possible is the preferred option, it is important to take into consideration the need for forensic work to determine how the system was compromised in the first place. Recovering a system too soon can often destroy the technical evidence of the attack. One option would be to put in place procedures and processes that allow you to preserve evidence offline while your system is being recovered.[40]

While taking that into account, there are certainly efforts that an organization can undertake in order to recover in a fast, safe and efficient manner. Through thorough business continuity planning, the organization will be better prepared for the recovery process (see section 4.0 Absorption).

As part of the recovery process, there should also be an investigation of the security incident itself. If the root causes of an attack are not addressed in a thorough manner, it could increase the probability of further and future compromise. Learning lessons from attacks, and mitigating where possible, is key after an organization has been attacked. The working group should also consider sanctions for users responsible for security infractions that led to an unwanted event.[41]

Basically, all of the universal mitigating mechanisms come into play in the recovery process, and a system with a high degree of adaptability will be able to recover sooner than a less adaptable one. The use of alternative backup solutions and redundant systems and infrastructure will

[40] Andress, Jason and Steve Winterfeld (2011):42
[41] Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b)

make recovery easier, and awareness among employees becomes increasingly relevant during a crisis. After going through business continuity planning and testing, it will also become clear where insurance policies are especially necessary.[42]

[42] Andress, Jason and Steve Winterfeld (2011):188

Annex A - Theoretical Principles and Key Definitions

This annex describes the theoretical principles and key definitions that form the conceptual basis of the methodology. It begins by clarifying what a methodology is, and how it differs from a method. It then moves on to discuss the challenges of performing risk assessments of cyber-related dependencies, vulnerabilities and threats. Finally, the concept of resilience is introduced and discussed as an alternative way of managing cyber security.

I. What is a methodology?

The terms "methodology" and "method" are often confused and used interchangeably. Yet there are significant conceptual differences between the two. In short, methodology is the science of methods. A methodology can be described as "a system of methods used in a particular area of study or activity", while a method can be described as "a particular procedure for accomplishing or approaching something".[43] In other words, while a methodology may incorporate several methods, and typically refers to the rationale and philosophical assumptions, or theoretical principles, of a particular study or activity, a method systematically details a given procedure, technique, or mode of inquiry.

These considerations have direct implications for the concept presented in this document. Methodologies pave the way for methods to be conducted properly. Methodology is the beginning whereas methods are the end of any scientific or non-scientific research. As such, there is a causal relationship between the two: The development of a methodology typically precedes the development of a method.

II. Risk assessment

The Oxford English Dictionary defines risk as: (Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility. Risk is however a contested concept, and there are several formulas and methods for identifying, calculating, qualifying, quantifying and rating risk. Risk analysis matured during the Cold War, and risk management has since become a popular activity in both private and public sectors, and many risk assessment methodologies and methods have already been developed for different purposes and organizations.

A risk formula usually consists of two or more variables that are weighted against each other, or multiplied, using some sort of quantitative or qualitative tool or model. Typical "ingredients" in a risk formula are probability and impact estimates, asset values, threats and vulnerabilities. A

[43] Oxford dictionary: http://oxforddictionaries.com/

common feature in all risk formulas is the need for reliable information on all variables. If too much information on one of the variables is lacking or uncertain, the risk measurement could end up without much value for the organization in question. When dealing with a fluid and dynamic threat environment such as the cyber domain, this is a fundamental challenge. In contrast to physical domains where military battles are traditionally fought (land, air and sea), the cyber domain is a man-made domain that is constantly growing and evolving. Due to its dynamic and composite nature, variables such as probability, impact, threats and vulnerabilities are extremely difficult to pinpoint and rate at any given moment. That is why traditional risk management methodologies may not be appropriate for managing cyber security, as is explained more in detail below.

Traditional approaches to risk assessments can roughly be divided into two categories:

1. Risk as the product of probability and impact
2. Risk as the product of assets value, threat and vulnerability

The first category is the most traditional way of estimating risk, and a number of methods exist that build on this approach. Some are purely quantitative where the variables "probability" and "impact" are quantified so that risk can be calculated, rated and presented numerically, while others are purely qualitative, using experts to determine levels of probability and likely impact. It is also common to determine an acceptable level of risk, so that the risk in any scenario that goes beyond that set level demands some sort of response.

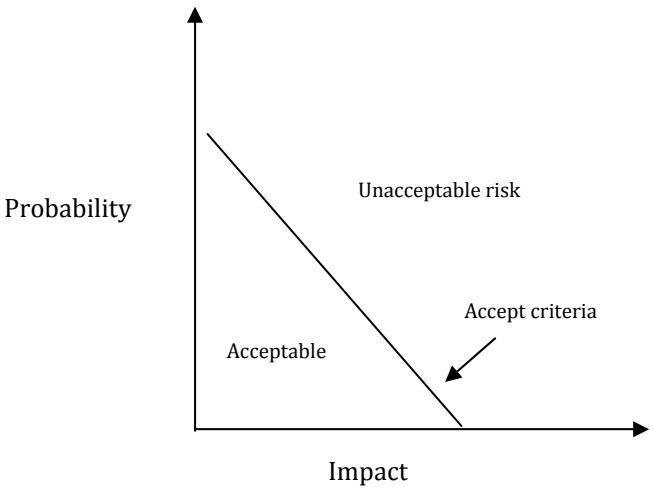


Figure 5. Risk Based on Probability and Impact

In a safety scenario one may assume that incidents will occur accidentally, and the use of stochastic methods using probability estimates may be valid. But in a security scenario which

only includes *intended* attacks that are not random, probability estimates lack validity because there are no reliable patterns that can be analyzed statistically.[44] Moreover, probabilities can only be based on past experience, and if there is one lesson to draw from history it is that strategic shocks and ruptures in trends are common. David Hume described this as the problem of induction – that we can never infer from the past to predict the future. In other words, estimating probabilities may not be a viable option when dealing with a volatile, fluid and rapidly evolving threat environment.

Another problem of using the probability and impact variables is the fact that not all threats can be known, especially in the cyber domain. That means that there are *unknown* threats for which you cannot estimate the probability or the impact, not to speak of the corresponding vulnerabilities.

Assessing the impact of *known* threats is also problematic when dealing with the cyber domain. First, there are so many interdependencies between cyberspace and other critical networks and infrastructures that it is extremely time-consuming and difficult to map out the casual relationships between them. Second, the issue of cascading effects is also of relevance as it is very hard to predict exactly where such effects might materialize.

Finally, there is the problem of how to weigh the probability and impact variables against each other. For instance, an attack with detrimental impact may be very unlikely and therefore score low in a risk estimate. At the same time, an attack with only moderate impact but high probability might score higher, depending on how probability and impact are weighted, a difficult problem to solve.

In conclusion, considering the problems outlined above, the probability/impact variables do not seem very useful for estimating risk when dealing with cyber security scenarios.

The second category of risk assessments sees risk as the product of assets values (or criticality), threats, and vulnerabilities. This understanding of risk may be more appropriate for the cyber domain because it does not include problematic concepts such as probability and impact. However, the challenge of having reliable data on all three variables, and of finding the appropriate way to weight them against each other, remains.

[44] Holm, Ola (2004): Safety scenarios include threats that are not intentional (e.g. accidents), in contrast to security scenarios which exclude unintentional threats.

According to this approach, risk is highest when criticality, threat and vulnerability intersect.[45]

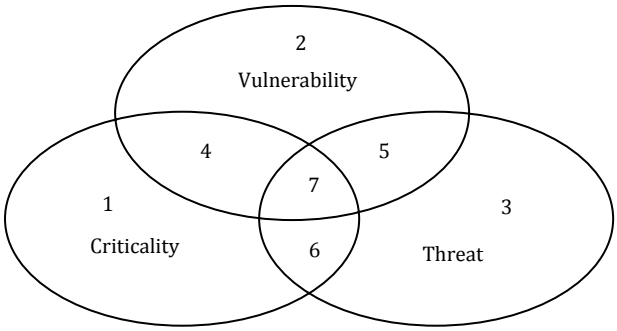


Figure 5 – Risk Based on Asset Value, Threat and Vulnerability

1. Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat.
2. Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there are no known threats.
3. Threat environments that have no critical assets or vulnerabilities (or vulnerability information).
4. Critical assets for which there are known vulnerabilities, but no known threat.
5. A threat or number of threats has acquired specific knowledge and/or capability to exploit vulnerability although not to critical assets.
6. Critical assets for which there are no known vulnerabilities, but there is exposure to a specific threat.
7. **Critical assets for which there are both known vulnerabilities and known threats. This is the most sensitive area.**

By including criticality as a key variable, this approach to risk assessment helps the user to identify key assets and functions. This is useful for prioritization of risk mitigating efforts because they will be based on known functionalities rather than on uncertain probabilities and impacts.

However, the problems of having reliable data on all variables and of weighing them against each other remain. One characteristic of the cyber domain is that new threats emerge continually at a rapid pace, making it hard to uphold a reliable threat picture. This rapid pace of

[45] Bass, Tim and Roger Robichaux (2001);
Holm, Ola (2004)

development could make cyberspace particularly prone to so-called Black Swan events.[46] Considering that vulnerability assessments are also normally based on existing threats, maintain a reliable vulnerability picture is equally as challenging.

In sum, this means that both types of risk assessment outlined above have inherent problems that will introduce difficulties when applying them to the cyber domain. It may therefore be a good idea to look for alternative approaches for managing cyber security.

III. Towards an alternative model for managing cyber security

The most important conclusion to draw from the discussion above is that it may be an overly ambitious task to calculate and rate risks when dealing with the cyber domain, at least when considering the time and resource constraints decision-makers are normally facing. This does not imply, however, that management of cyber security is an impossible task. What it does imply is the need to look for alternative and possibly less ambitious models or methodologies.

Amongst the various steps in the traditional risk management models some come across as more manageable than others. Identifying key assets and mapping dependencies seem to be easier than identifying threats, and estimating probabilities and impact. Carrying out a vulnerability analysis may also be easier than carrying out a threat analysis. After all, most organizations know themselves better than they know their adversaries. More importantly, collecting information about your own organization is easier than collecting information about known and unknown adversaries with both known and unknown capabilities and intentions. Threats are often beyond our reach, vulnerabilities are usually self-generated.

IV. Critical assets

The first step in any security management process should be to identify the critical assets and functions of the nation or organization at hand. If you do not know what to protect and why, there is no point in analyzing dependencies, threats and vulnerabilities. Governments have recently expanded their views on what is considered critical infrastructure, moving from focusing on the adequacy of a nation's public works, to including a wide range of both public and private sectors. Overviews of what is considered critical assets and functions are expected to continue to evolve as geopolitical or economic changes occur. For a nation, critical infrastructure

[46] A Black Swan is an event with the following three attributes: "First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable." -*The Black Swan: The Impact of the Highly Improbable* from Andress, Jason and Steve Winterfeld (2011):257.

can include communications, emergency services, energy, finance, food, government and public services (including defense), health, transport, and water.[47]

Most nations and organizations have to accept that not all assets can be equally secure and that a prioritization of efforts is necessary. In order to prioritize, it is necessary to identify the assets, infrastructures and functions that are essential for maintaining a stable condition. The criticality analysis results in identifying all critical processes in an organization and portraying their sub-processes as well as their "risk elements". Risk elements can include people, facilities and equipment, data and files, grounds and buildings, as well as other resources. The nation or organization should decide which criteria to use in the analysis, how many criteria should apply at once and what classification to use within the criteria.

V. Dependencies

Once you know what your critical assets are, it is possible to start investigating whether and how these assets, infrastructures and functions depend on the cyber domain, directly or indirectly. Dependency is the relationship between two structures or functions in which one is required for the generation of the other.

Modern societies use the cyber domain to communicate, to deliver services, and to store information to meet official, commercial and personal needs; the cyber domain is now ubiquitous and essential. Cyber dependencies have reached the point where alternatives no longer exist or can only be provided at great cost and after substantial time lapses. Cyber dependencies can therefore be viewed as a specific type of vulnerability.

Infrastructure systems are characterized by a high degree of interconnection, and the functioning of one service often depends on the functioning of another. Services can also be mutually dependent on each other to function, exhibiting interdependence. In addition, services are implemented across a range of contractual, organizational, commercial, legal and political boundaries giving rise to a complex set of ownerships and responsibilities. This provides further possible coupling and dependencies due to for example organizational or maintenance deficiencies, or operational constraints of failure or isolation.

Such interconnection can in many cases be measured only in qualitative terms. Many physical, virtual and logical dependencies are not apparent until a crisis occurs and the connection breaks

[47]Moteff, John, Claudia Copeland, and John Fischer (2003);
Moteff, John and Paul Parfomak (2004);
Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke (2011)

down. The high level of interdependence can lead to cascading shut-downs. At the same time, smaller and smaller disruptions are enough to cause dramatic consequences in complex systems (this is called the vulnerability paradox).

VI. Vulnerabilities[48]

A vulnerability can be described as a weakness in a system which reduces the ability to manage unwanted events and/or recover from them, and a threat needs a corresponding vulnerability to be able to materialize in a system. Vulnerabilities can be technical in nature, but could equally be people, process, structure or policy-related, and/or be due to a natural hazard or man-made action. To fully understand all vulnerabilities, all components of the potential target system and the interactions between them need to be considered.

When we say that critical infrastructure is dependent on the cyber domain, we often mean dependent on the Internet or networks using that same technology. This means that the same vulnerabilities we know from the Internet or other connected systems are also applicable to parts of critical infrastructures. For information and communications technology systems one can divide vulnerabilities into four classes: Vulnerabilities due to errors made in the design, implementation, configuration, or use of the technology. A more generic approach is to explore physical, logical and social vulnerabilities on different layers of the cyber domain: users, applications, fundamental services, and communications infrastructure (see Table 2).

At the user layer typical malware threats and software vulnerabilities are perhaps the most prominent. As an example, Stuxnet exploited vulnerabilities at this layer to attack critical infrastructure in Iran. At the application layer we find some of the most widespread means of communication and channels for informing the public. Attacks against these can either hinder or disrupt the communication, both internally in a key societal function, or by misinforming or denying information to the public. At the lower layers we find the fundamental services and the communications infrastructure (transmissions, transport and access networks) that offer services upon which the higher level functions depend. Vulnerabilities in these could potentially affect many systems. While many believe these layers are mature and not as prone to design and implementation errors, configuration errors made by an organization may open the organization up to an attacker.[49]

[48] This section is based on Fridheim, Håvard and Janne Hagen (2007) and BAS 5-prosjektet (2007).
[49] Fridheim, Håvard and Janne Hagen (2007);
BAS 5-prosjektet (2007)

In addition to the technical vulnerabilities mentioned above, an important aspect is the policy enforced on the users and systems. Policy can help mitigate many of the social vulnerabilities, for instance by prohibiting the use of USB memory sticks for systems handling critical infrastructure.

The list of possible vulnerabilities however is long and ever changing. It is however important to note that vulnerabilities are not solely "inadequacies" in a system, as the attribute representing a vulnerability could be among the most positive attribute of an asset. For example, the portability of laptop computers, a positive feature of the asset, increases the likelihood of theft.[50]

VII. Threats

The problem with threats in cyberspace is that you are often not aware of them before it is too late. Threat is typically defined as the product of (bad) intention and capability. However, these two variables seldom operate together in the open, and it may therefore be hard to generate a reliable threat picture.

There is little point in trying to predict the next attack in anything but the most generic terms. If an attacker wants to attack networks/infrastructure/other cyber assets, he will attempt to do so in a way that has not been seen before. It may however be useful to categorize threat actors as a more general projection of the threat picture. In the cyber domain, we typically refer to the following categories of threat actors: Criminal Groups; Hackers; Hacktivists; Insiders; National Governments and Foreign Intelligence Services; and Terrorist Groups. These groups can have widely different motives for attacking an organization's key assets. For example, criminal groups are usually financially motivated, seeking economic gains through illicit action. Terrorists however seek to create fear and destruction, often with a political end-goal. Due to the wide range of actors and motives, combined with a rapidly changing technological environment, it is very difficult to gain complete oversight when it comes to cyber threats.[51]

VIII. Resilience: because deterrence is not enough

Once critical dependencies and vulnerabilities are identified, and are seen in the context of an updated threat picture, the decision-maker must consider what measures are most appropriate for reducing both dependencies and vulnerabilities. This is where the concept of *resilience* becomes relevant. As explained below, there are in fact universal mitigating measures with "guaranteed effect" that can be considered against factors such as cost and time. In some cases, however, these universal mechanisms may not be sufficient for handling the problem, and the

[50] Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b):6
[51] Multinational Experiment 7 – Objective 3.1 Workshop Input from Spain (2012)

decision-maker must consider whether a deeper analysis is needed to uncover the more technical aspects of given dependencies and vulnerabilities. At this point, the purpose of this particular methodology ends as it cannot go into the technicalities of cyber security. However, it will have helped the decision-maker identify the need for deeper analysis, and made him or her aware of a critical dependency and/or vulnerability.

Just like risk, resilience is a contested concept. It is a term with many connotations, but with few clear definitions. Yet, a lot of thorough and innovative work has been done in recent years, especially in the United States, on developing a common understanding of resilience from a national security perspective.[52] The understanding of resilience presented here builds on this work, in addition to insights emerging from MNE 7 workshops and activities.

Resilience can be viewed as an alternative to classic deterrence or as a complementing effort.[53] Deterrence is the ability to persuade a potential aggressor that the costs and risks of attacking will outweigh the gains. Given rationality, the aggressor will refrain from attacking. Resilience, in contrast, is about accepting the risk of an attack taking place, and focusing on strengthening the ability to prevent, detect, absorb and recover from an attack, enabling an organization to maintain capability or services at an acceptable level throughout an attack cycle.[54]

The reason why resilience might be a better defense strategy when dealing with the cyber domain, is that it is highly likely that attacks will be carried out notwithstanding attempts to deter or protect against them. By focusing on resilience, we acknowledge that the risk of being attacked in the cyber domain is very high, and that the possibility of eliminating all threats is very low due to its composite, rapidly evolving and unpredictable nature. Therefore, instead of dealing with the threats directly, we choose instead to manage them through strengthening our resilience, i.e. our ability to prevent, detect, absorb and recover from attacks. These key terms represent our understanding of resilience.

Prevention can be active or passive. Active prevention can be interdiction or elimination of known threats before an attack is launched, which requires detailed pre-knowledge about the

[52] Palin, Philip J. (2009);
Palin, Philip J. (2010);
US White House (2011);
US Department of Defense (2011);
US Department of Homeland Security (2010a);
US Department of Homeland Security (2010b)
[53] Although resilience can be viewed as an alternative to deterrence, it can also function as a deterrent; if you can demonstrate your system to be highly resilient, adversaries are less likely to attack it.
[54] Critical Infrastructure Protection Program (2007)

threats. Passive prevention can be the creation of firewalls and using antivirus software, building cyber security awareness or reducing dependencies between the cyber domain and other critical infrastructures and functions. This concept will mainly deal with passive prevention mechanisms, as it is both "non-technical" and unclassified in nature.

Detection is about being able to detect an attack as soon as possible, and about having the policies in place to deal with an attack as effectively as possible. If an attack is not detected, the system will not have the chance to absorb and recover from the attack. This can have great consequences.

Absorption is about creating damage-tolerant systems that serve to contain, soak-up or deflect the consequences of an attack. It also allows decision-makers to "cut some slack" in their response to a cyber attack, i.e. allowing for enough time to analyze the problem before a critical decision must be made on how to respond to it.

Recovery is about the ability to effectively "bounce back" to a stable condition after an attack has been launched. It is worth noting that recovery can be much more than simply restoring or repairing physical and technical damages. Recovery also has a social dimension which can be equally or more difficult to restore.

Mitigating mechanisms

There are many ways and means to strengthen resilience. Some are context-sensitive, meaning that they work in some cases and not in others, while others are more generic or universal, meaning that they will have an effect regardless of the types of threat or attack one is dealing with. For the purpose of this methodology, which is meant to be generic, we will focus on those universal mitigating mechanisms that will always have a positive effect on strengthening resilience. We have identified 7 such mechanisms:

1. Building awareness
2. Reducing dependencies
3. Increasing redundancy
4. Developing alternative back-up solutions
5. Increasing adaptability
6. Transferring risk
7. Sharing information

Much can be said about each of these mechanisms. We will not provide a detailed discussion of them here, but rather briefly explain their inner logic.

Building awareness rests on the assumption that people represent a fundamental vulnerability to cyber security. By raising the level of cyber security awareness among people in nations and organizations, the risk of being the target of a successful cyber attack will likely be reduced.

Reducing dependency of critical infrastructures on the cyber domain will ensure a reduction in the risk of being impaired by cyber attacks. One problem is that by reducing such dependencies you are also likely to reduce functionality and the effectiveness of these systems. One will therefore have to do a cost-benefit analysis to consider whether this type of mitigating measure is worth the risk reduction. Its strength lies in the fact that a 100% reduction of dependency equals a 100% reduction of risk.

Increasing redundancy is about creating a surplus of capacity in a system, structure, function or capability so that a reduction of performance caused by a cyber attack will be compensated for by the spare capacity.

Developing alternative back-up solutions is about using different means to reach the same end or maintain the same function. In contrast to redundancy in which you have more of one capacity, this mitigating measure focuses on developing alternative ways of serving a specific function. For example, in an aircraft a pilot may have one inertial navigation platform, but for redundancy he would have two or more, just in case one fails. However, as alternative back-up solutions he would carry a map and stopwatch and look out the window, in case all of the navigation platforms are disrupted simultaneously.[55]

Increasing adaptability is about being able to adapt to a constantly evolving domain such as cyberspace. "A resilient system is one that fluctuates because it responds and adjusts to internal and external change. In this regard, resilience is qualitatively different from stability and sustainability, which are merely aspects of equilibrium."[56]

Transferring risk is one way of planning for effective recovery after an attack, for instance through insurance. It does not necessarily have to be about financial insurance. It can also be

[55] A similar concept is "Defense in Depth", see Andress, Jason and Steve Winterfeld (2011):189.
[56] JHSEM:16

bilateral or multilateral agreements between partner nations and/or organizations which oblige them to help each other physically, technically, socially or financially in case of an attack.

Sharing information is becoming increasingly important as actors are realizing that one cannot predict all threats in cyber space. By pooling knowledge and receiving/providing advice organizations can become more aware of the concrete actions they can take to become more resilient. Accurate and timely situational awareness, both during normal activity and when anomalies are detected, will increase the level of resilience.[57]

[57] Multinational Experiment 7 – Objective 3.2 Concept (2012)

Annex B – Ten Commandments of Resilience

I. Make resilience a priority

II. Know yourself, as you cannot know others

III. Know what you depend on, and reduce those dependencies

IV. Know where you are vulnerable, and patch those vulnerabilities

V. Build awareness in your organization

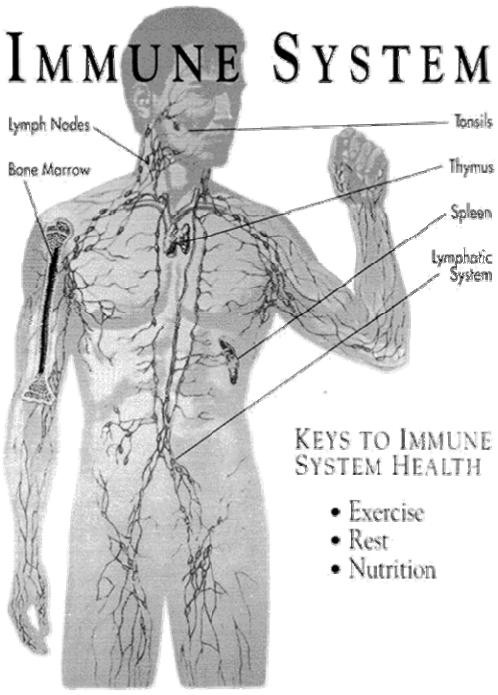
VI. Increase redundancy in your systems

VII. Have alternative back-up systems in place

VIII. Be able to adapt to rapid changes in your environment

IX. Transfer risk away from your key assets

X. Share information



Annex C - Methodology Crosswalk

Step	Activity/Task	Section/Page
PREVENTION		
Establish Working Group		1.0/4
1	Define scope/boundaries of analysis	1.0/4
2	Determine skill sets, knowledge, and expertise required	1.0/4
Outputs: • Mandate • Member list • Schedule		
Identify Critical Assets		2.1/6
3	Establish criticality criteria (for prioritization)	2.1/6
4	Identify mission critical capabilities and services	2.1/6
5	Identify key processes required to produce 2.2	2.1/6
6	Identify key assets required to support 2.3	2.1/6
Outputs: • Prioritized list of mission critical capabilities and services (and the critical processes and assets which support the provision of these)		
Conduct Dependency Analysis		2.2/7
7	Conduct supply chain analysis	2.2.1/7
8	Conduct value chain analysis	2.2.1/7
9	Identify critical dependencies on cyberspace (downstream and upstream in the organization)	2.2.1/7
10	Prioritize critical dependencies (identify those requiring of mitigation)	2.2.2/8
Outputs: • Prioritized list of dependencies (upstream and downstream) • List of critical dependencies in immediate need of mitigation		
Conduct Vulnerability Analysis		2.3/9
12	Identify vulnerabilities	2.3.1./10
13	Analyze the impact of an unpatched vulnerability	2.3.2/11
14	Assess which vulnerabilities need mitigation	2.3.3/12
Outputs: • Prioritized list of vulnerabilities • List of critical vulnerabilities in immediate need of mitigation		
Conduct Threat Analysis		2.4/13
15	Analyze previous attempted and/or successful cyber attacks against your organization in search of identifiable threat actors	2.4/13
16	Identify categories of threat actors relevant for your organization	2.4/13

17	Identify motivations and modus operandi for known threats	2.4/14
18	Identify what other actors know about your organization	2.4/14
19	Identify which known threat actors and behaviors you can mitigate	2.4/14
Outputs: • List of known threats to your organization • Overview of the expected behavior of known threat actors • Contingency plans for known threats		
DETECTION		
20	Find mean time from attack occurs until it is detected	3.0/15
21	Identify incident/attack reporting routines in the organization	3.0/15
22	Identify information sharing frameworks and routines (for sharing with other organizations/actors/government agencies)	3.0/15
23	Assess whether these routines could be improved upon	3.0/16
Outputs: • Measure of detection efficiency • Overview of incident/attack reporting routines (and where mitigating measures are required in order to improve) • Overview of information sharing frameworks and routines (and where mitigating measures are required in order to improve)		
ABSORPTION		
24	Identify what is done technically to absorb a cyber attack (by using technical expertise)	4.0/16
25	Identify key processes and personnel involved in absorption	4.0/16
26	Create business continuity plan	4.0/17
27	Test business continuity plan	4.0/17
28	Improve business continuity plan	4.0/17
Outputs: • Overview of processes and procedures for management of the absorption process, both in terms of technical staff and others (and where mitigating measures are required in order to improve upon these processes) • Tested and improved business continuity plan		
RECOVERY		
29	Identify authority to “clear” a compromised system for use	5.0/18
30	Identify procedures for post-attack forensics	5.0/18
31	Identify procedures for after-action reports and lessons learned activities	5.0/18
Outputs: • Overview of the chain of command in the recovery process (and where mitigating action is needed) • Overview of the processes for after-action reporting and learning of lessons (and where mitigating action is needed)		

Bibliography

Andress, Jason and Steve Winterfeld (2011). *Cyber Warfare – Techniques, tactics and Tools for Security Practitioners*, Waltham, MA: Syngress.

Audestad, Jan (2005). *E-bomber og E-granater – Om IKT og sårbarhet*. FFI-note 2005/00938, Kjeller.

Aven, Terje (2006). "A unified framework for risk and vulnerability analysis covering both safety and security", *Reliability Engineering and System Safety* 92, 745–754.

BAS 5-prosjektet (2007). *Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT*. SEROS report nr. 91892.

Bass, Tim and Roger Robichaux (2001). "Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations", *IEEE MILCOM 2001*, http://www.thecepblog.com/papers/pdf/archives/defense-in-depth-revisited-original.pdf.

Brown, Gerald, Matthew Carlyle, Javier Salmerón, and Kevin Wood (2006). "Defending Critical Infrastructure". *Interfaces* 36(6):530-544.

Chittister, Clyde G. and Yacov Y. Haimes (2011). "The Role of Modeling in the Resilience of Cyberinfrastructure Systems and Preparedness for Cyber Intrusions", *Journal of Homeland Security and Emergency Management* 8(1), Article 6, http://www.bepress.com/jhsem/vol8/iss1/6/.

Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke (2011). *Cyber Security and the UK's Critical National Infrastructure*. Chatham House Report, September 2011, http://www.chathamhouse.org/publications/papers/view/178171.

Critical Infrastructure Protection Program (2007). *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. CIPP Discussion Paper Series, February 2007, George Mason University School of Law, http://cip.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf.

CSIS Commission on Cybersecurity for the 44th Presidency (2011). *Cybersecurity Two Years Later*. Report. Center for Strategic & International Studies, January 2011, http://csis.org/publication/cybersecurity-two-years-later.

Danish Emergency Management Agency (2006). *Introduction and user Guide: DEMA's Model for Risk and Vulnerability Analysis*. DEMA 2006, http://brs.dk/eng/inspection/contingency_planning/rva_model/Pages/rva_model.aspx.

Deibert, Ronald J. and Rafal Rohozinski (2010). "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology* 4, 15-32.

Demchack, Chris C. (2012) "Resilience, Disruption and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World". In Burns and Price (eds.) *Securing Cyberspace: A New Domain for National Security,* Washington, DC: The Aspen Institute

DEU Federal Ministry of the Interior (2011). *Cyber Security Strategy for Germany*. Berlin, February 2011, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

Feller, Andrew, Dan Shunk, and Tom Callarman (2006). "Value Chains Versus Supply Chains" *BPTrends* 3.

Ford, E. T. Aven, H. Wiencke and W. Røed (2007). "An approach for evaluating methods for risk and vulnerability assessments", in Aven and Vinnem (eds.) *Risk, Reliability and Societal Safety*, London: Taylor & Francis group.

Fridheim, Håvard and Janne Hagen (2007). *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport*. FFI-report 2007/01204, Kjeller, http://rapporter.ffi.no/rapporter/2007/01204.pdf.

Geers, Kenneth (2011). *Strategic Cyber Security*. NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), Tallinn, http://www.ccdcoe.org/278.html.

Gibb, Forbes and Steven Buchanan (2006). "A framework for business continuity management" *International Journal of Information Management* 26:128-141

Hagen, J.M., B.O. Knutsen, T. Sandtrup and M. Bjørnenak (2011) "How the use of modeled scenarios can improve risk awareness and risk control in complex environments", Research Paper, Norwegian Defence Research Establishment, Kjeller 2011.

Hollnagel, Erik, David D. Woods and Nancy Levenson (2006). *Resilience Engineering*. Aldershot: Ashgate Publishing Limited.

Holm, Ola (2004). *Risikohåndtering av informasjonssystemer I dynamiske omgivelser*. Master's Thesis in Information Security. Gjøvik: Høgskolen i Gjøvik.

Hunker, Jeffrey (2010). "Cyber war and cyber power: Issues for NATO doctrine", *NATO Research Paper* 62, November 2010, Research Division – NATO Defence College, Rome, http://www.europesworld.org/NewEnglish/Home_old/PartnerPosts/tabid/671/PostID/2030/language/en-US/Default.aspx.

Information Assurance Technology Analysis Center (2009). *Measuring Cyber Security and Information Assurance*. IATAC State-of-the-Art-Report (SOAR), 8 May 2009, http://iac.dtic.mil/iatac/download/cybersecurity.pdf.

Jackson, Scott (2010). *Architecting Resilient Systems*. Hoboken, NJ: John Wiley & Sons.

Jasper, Scott (2010). *Securing Freedom in the Global Commons.* Stanford, CA: Stanford University Press.

Joint Chiefs of Staff (1997). *Joint Doctrine for Operations Security*. Joint Pub 3-54, 24 Jannary 1997, http://www.bits.de/NRANEU/others/jp-doctrine/jp3_54rfd.pdf.

Jones, Andrew (2002). *Identification of a Method for the Calculation of Threat in an Information Environment*. University of Glamorgan, April 2002, http://people.emich.edu/pstephen/E_M_U_files/Cybercrime-1/Threat-Method-Phase-1.pdf.

Kahan, Jermoe H., Andrew C. Allen and Justin K. George (2009). "An Operational Framework for Resilience", *Journal of Homeland Security and Emergency Management* 6(1), Article 83, http://www.bepress.com/jhsem/vol1/iss1/83/.

Kontio, Jyrki, Gerhard Getto and Dieter Landes (1998). "Experiences in improving risk management processes using the concepts of the Riskit method". Paper presented at the SIGSOFT'98 Sixth International Symposium of the Foundation of Software Engineering, November 3–5, 1998, http://dl.acm.org/citation.cfm?id=288301.

Lewis, James Andrew (2010). "The Cyber War Has Not Begun", Commentary, Center for Strategic International Studies, March 2010, http://csis.org/publication/cyber-war-has-not-begun.

Luiijf, H., K. Besseling, M. Spoestra and P. de Graaf (2011). "Ten National Cyber Security Strategies: a comparison". Research Paper, Netherlands Organisation for Applied Scientific Research (TNO).

MacIntosh, JP. J. Reid and LR. Tyler (2011). *Cyber Doctrine: Towards a coherent evolutionary framework for learning resilience*. Institute for Security & Resilience Studies, June 2011, http://www.ucl.ac.uk/isrs/publications/CyberDoctrine.

Masters, Jonathan (2011). "Confronting the Cyber Threat", *Backgrounder*, Council on Foreign Relations, 23 May 2011, http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577.

Mayron, Liam M., Gisela Susanne Bahr, Carey D. Balaban, Matthew G. Bell, Richard Ford, Kevin L. Fox, Ronda R. Henning, and Wayne B. Smith (2010). "A Hybrid Cognitive-Neurophysiological Approach to Resilient Cyber Security", paper presented at the 2010 Military Communications Conference,

http://202.194.20.8/proc/MILCOM2010/papers/p1794-mayron.pdf.

McCreight, Robert (2010). "Resilience as a Goal and Standard in Emergency Management", *Journal of Homeland Security and Emergency Management* 7(1), Article 15, http://www.bepress.com/jhsem/vol7/iss1/15/.

Mørkestøl, Kristin and Lene Bogen (2006). *ICT Crisis Management – Actors and Roles*. FFI-report 2006/00245, Kjeller, http://rapporter.ffi.no/rapporter/2006/00235.pdf.

Morozov, Evegeny (2010). "Battling the Cyber Warmongers", *The Wall Street Journal*, 8 May 2010, http://online.wsj.com/article/SB10001424052748704370704575228653351323986.html.

Moteff, John, Claudia Copeland, and John Fischer (2003). *Critical Infrastructure: What makes an Infrastructure Critical?* Report for Congress, Congressional Research Service, Library of Congress, USA.

Moteff, John and Paul Parfomak (2004). *Critical Infrastructure and Key Assets: Definition and Identification.* Report for Congress, Congressional Research Service, Library of Congress, USA.

Multinational Experiment 7 – Objective 3.1 Workshop Input from Austria (2011). *"Mapping Exercise - Austria".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011a). *"Mapping Exercise".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from Canada (2011b). "Identifying Network Vulnerabilities".

Multinational Experiment 7 – Objective 3.1 Workshop Input from Germany (2011). *"Case Study - Identifying Asset Values/Criticalities".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from Germany (2012). *"Case Study on Relevant Cyber Dependencies, Threats and Vulnerabilities of the Federal Republic of Germany".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from Poland (2011). *"Mapping Exercise - Poland".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from Spain (2011*). "Spanish Mapping Exercise".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from Spain (2012). *"Threat Analysis".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from the United Kingdom (2011a). *"(Inter) Dependency Analysis".*

Multinational Experiment 7 – Objective 3.1 Workshop Input from the United Kingdom (2011b). *"Mapping Exercise".*

Multinational Experiment 7 – Objective 3.2 Concept (2012). *"Information Sharing Framework".*

Nasjonal sikkerhetsmyndighet (2006). *Veiledning i risiko- og sårbarhetsanalyse*. NSM 5 December 2006, https://www.nsm.stat.no/Documents/Veiledninger/ROS_2004_veiledning.pdf.

National Infrastructure Advisory Council (2009). *Critical Infrastructure Resilience Final Report and Recommendations*. NIAC 8 September 2009, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

Nystuen, Kjell Olav and Håvard Fridheim (2007). *Sikkerhet og sårbarhet i elektroniske samfunnsinfrastrukturer – refleksjoner rundt regulering og tiltak*. FFI-report 2007/00941, Kjeller, http://rapporter.ffi.no/rapporter/2007/00941.pdf.

Palin, Philip J. (2009) "Resilience Policy Directorate: important, urgent and open to definition", *Homeland Security Watch* 2 June 2009, http://www.hlswatch.com/2009/06/02/resilience-policy-directorate-important-urgent-and-open-to-definition/.

Palin, Philip. J. (2010). "Resilience: The Grand Strategy", *Homeland Security Affairs* 6(1), http://www.hsaj.org/?article=6.1.2.

Payne, Shirley C. (2006). "A Guide to Security Metrics", SANS Security Essentials GSEC Assignment Version 1.2, SANS Institute 2007, http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.

Per Concordian: Journal of European Security and Defense Issues 2(2). "Securing Cyberspace".

Ralston, P.A.S., J.H. Graham and J.L. Hieb (2006). "Cyber security risk assessment for SCADA and DCS networks", *ISA Transactiuons* 46, 583–594, ftp://163.25.117.117/gyliao/TODylan/Cyber%20security%20risk%20assessment%20for%20SCADA%20and%20DCS%20networks.pdf.

Recipe (2011). *Good Practices Manual for CIP Policies*. Netherlands Organisation for Applied Scientific Research (TNO), http://www.tno.nl/recipereport.

Schrader, Dennis R. (2010). "The New Preparedness of Challenge: Transitioning Resilience from Theory to Reality", *DomesticPreparedness.com*, 10 February, 2010, http://www.domesticpreparedness.com/Infrastructure/CIP-R/The_New_Preparedness_Challenge%3A_Transitioning_Resilience_from_Theory_to_Reality/.

Sivertsen, Tormod Kalberg (2007). *Risikoanalyse av samfunnskritiske IKT-systemer*. FFI-report 2007/00910, Kjeller, http://rapporter.ffi.no/rapporter/2007/00910.pdf.

Skillinghaug, Arild (2011). *Fortsatt ansvarsprinsipp eller helhetlig tilnærming til cybersecurity i Norge?* Master's Thesis. Norwegian Defence and Staff College, spring 2011, http://brage.bibsys.no/fhs/handle/URN:NBN:no-bibsys_brage_18074.

Stanton, Ray (2005). "Beyond Disaster Recovery: the Benefits of Business Continuity" *Computer Fraud & Security* 8(7):18-19

Swaminathan, Jayashankar M, Stephen F. Smith, and Norman M. Sadeh (1998). "Modeling Supply-Chain Dynamic: A Multiagent Approach" *Decision Sciences 29(3)*

Thuv, Aasmund, Ronny Windvik, Kjell Olav Nystuen og Tormod Sivertsen (2007). *Sårbarheter i Internett*. FFI-report 2007/00903, Kjeller, http://rapporter.ffi.no/rapporter/2007/00903.pdf.

UK Cabinet Office (2009). *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*. UK Office of Cyber Security & UK Cyber Security Operations Centre, June 2009, http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

US Department of Defense (2011). *Department of Defense Strategy for Operating in Cyberspace*. DoD, July 2011, http://www.defense.gov/news/d20110714cyber.pdf.

US Department of Homeland Security (2010a). *Bottom-Up Review*. DHS, July 2010, http://www.dhs.gov/xlibrary/assets/bur_bottom_up_review.pdf.

US Department of Homeland Security (2010b). *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. DHS, February 2010, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

US White House (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Verton, Dan (2003). *Black Ice: the Invisible threat of Cyber-Terrorism*, Emeryville, CA: McGraw-Hill

Wallace, Michael and Lawrence Webber (2010). *The Disaster Recovery Handbook: A Step by Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities and Users.* New York, NY: AMACOM

Wiencke, H.S., T. Aven and J. Hagen (2006). "A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on information and communication technology", in Guedes Soares and ZIO (eds.) *Safety and Reliability for Managing Risk*, London: Taylor Francis Group.

Wilson, Clay (2007). *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. Report for Congress, Congressional Research Service, Library of Congress, 20 March 2007, http://www.fas.org/sgp/crs/natsec/RL31787.pdf.

Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands.

Zavidniak, Paul, Anita D'Amico and Dennis H McCallam (1999). "Achieving Information Resiliency". *Information Technology Security Report* 4(3), 54–62, http://www.securedecisions.com/wp-content/uploads/2011/06/Achieving-Information-Resiliency.pdf.