Cyber Israel
Prime Minister's Office
National Cyber Directorate

NATIONAL CYBER CONCEPT FOR CRISIS PREPAREDNESS AND MANAGEMENT

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The rise in the capabilities and efforts of attackers in cyberspace, concurrent with the growing dependence on computerized systems, significantly increases the likelihood that a *widespread persistent cyber crisis* will materialize, with the potential of causing enormous damage to organizations, sectors and even to countries.

In order to effectively contend with a cyber crisis, preliminary preparations are necessary. Such actions will enable crisis management for the sake of mitigating damages, ramifications and shorten crisis duration. Therefore, within the scope of its efforts to build national cyber robustness and resilience, the Israeli National Cyber Directorate (INCD) is promoting the subject of cyber crisis preparedness. A material component of these preparations is the **"National Cyber Concept for Crisis Preparedness and Management"**, which is presented hereunder.

The National Cyber Concept is a fundamental basis that defines principles and modes of action on the subject of crisis preparedness and management in civil cyberspace. It provides a framework for a common language, and deepens the cooperation on the subject of cyber crises for government ministries, regulatory authorities, state cyber-security organizations and for the entire economy.

It also serves as a tool that every organization can use in building a cyber crisis preparedness and management plan, each at its level, in order to maintain functional and business continuity, and helps organizations ascertain the extent of their organizational preparedness in this regard. The National Cyber Concept defines how to map "vital cyber assets", describes cyber states of alert and principles for changing the level of alert, and elaborates on the subjects of assembling a preparedness "toolbox", the cyber crisis management concept, and actions that will help contend adequately with the crisis.

Considering the grave repercussions of a cyber crisis, and since it is not only a technological issue, but rather is a complex issue requiring responses from many functionaries and the development of suitable organizational capabilities, the National Cyber Concept is intended for boards of directors and managements of organizations, since they bear the overall responsibility for crisis preparedness and will be managing the crisis, if it materializes. The National Cyber Concept is also intended for managers of cyber defense and emergency preparedness, and for those responsible for risk management, functional and business continuity.

The National Cyber Concept was written at the National Preparedness Center in the INCD, based on the knowledge and experience amassed at the INCD and at cyber-security organizations in the public and private sectors in Israel and abroad. Procedures and work methods will be disseminated in the future based on the National Cyber Concept, as well as documents providing in-depth professional information on the subject of cyber crisis preparedness and management, which should help assimilate and implement the National Cyber Concept in the Israeli economy.

2. TERMS AND DEFINITIONS

The terms and definitions below are based on the "cyber glossary"[1] prepared at the INCD, and on government resolutions and documents addressing emergency preparedness.

Global cyberspace: the compound of information technology infrastructure, which includes the internet, communications networks, computerized systems and all computerized processors and controllers embedded in technological systems, and the users of all of these.

Israel's civil cyberspace: the cyberspace of all governmental and private parties in the State of Israel, excluding particular entities (the Israel Defense Forces, the Israeli Police, Israel Security Agency, the Institute for Intelligence and Special Operations, and the Defense Establishment).

Cyber asset: teleprocessing systems (both hardware and software) that is used, inter alia, for storing, managing, processing and transmitting information and/or for operations, command and control.

Vital cyber asset: a cyber asset whose normal functioning is essential for maintaining the continuity of a core process.

Core process: a process being carried out by an organization in order to achieve its key objectives and/or objectives that have been defined for that organization.

Cyber routine: normal situation with no indication of damage to the normal functioning of vital cyber assets.

Cyber incident: an occurrence that indicates possible damage to the normal operation of a cyber asset, when it is reasonable to assume that it derives from a deliberate activity in cyberspace.

Cyber crisis: a situation posing a real threat of damage, or actual damage, to a vital cyber asset, which is liable to cause critical damage to routine operations, reputational damage, economic damage and endanger human lives. A cyber crisis has varying degrees of gravity and, in an extreme situation, substantial damage is caused to core processes and to the functional continuity of an organization/the economy, which is liable to escalate to the point of a national state of emergency.

Emergency trigger: warfare, natural phenomenon, cyber crisis, terrorist activity, malfunction, etc., whose inherent risk has been assessed as being liable to trigger an emergency.

National state of emergency: a grave and dangerous situation posing a real risk of harm to the public and/or to the state's national resilience, which necessitates multi-disciplinary action at the national level, including a declaration by law (such as: a "special home front situation", "civilian emergency event," a declaration of war).

National state of alert:[2] derives from the possibility of an emergency occurring, the results of which cross organizations. The purpose of declaring a national state of alert is to reduce the likelihood of an event occurring and the potential damage resulting from its occurrence. A national state of alert necessarily affects the cyber state of alert.

Cyber state of alert: an official determination about the nature, level and scope of the cyber preparedness that is needed in order to contend with the circumstances. A cyber state of alert may affect the national state of alert.

[1] The glossary can be found on the INCD website: https://www.gov.il/he/Departments/General/terms.

[2] The terms "national state of emergency" and "national state of alert" have not yet been defined in law.

3. INTRODUCTION

3.1 The efforts to protect civil cyberspace

Over the past decade, we have been witnessing the tremendous development of cyberspace and the variety of opportunities and possibilities that it offers. At the same time, the accelerated growth of attack technologies and the growing dependence on the use of computerized systems, have also led to the exploitation of cyberspace as an expansive medium for hostile activities that are steadily increasing in intensity and in magnitude. Cyber assets, particularly critical infrastructures (CI), have become high-quality targets for attacks and the number and types of targets are steadily growing, and as a result, so is the danger posed to private individuals, organizations, sectors and countries.

According to the aggregate threat scenario for the civilian arena, which was approved by the Security Cabinet of Israel in Resolution B/120,[3] cyberspace is a major emergency trigger that is liable to lead to a national emergency. Accordingly, in Resolutions 3611[4] and 2444,[5] the government addressed the need to formulate a national concept for dealing with emergency situations in cyberspace, adding that ensuring the safe and normal functioning of cyberspace is needed routinely and during emergencies, and that this is a national interest and objective that is critical to the security of the State of Israel.

Considering the volatile potential of the cyber threat and the government's instructions in this regard, the Israeli National Cyber Directorate (INCD), in collaboration with government ministries, and with the assistance of regulatory authorities and other government organizations, is leading the efforts to protect Israel's civilian cyberspace and to keep it at a safe distance. The efforts focus on taking actions to provide guidance and instruction to organizations in the economy, based on the understanding that, in many instances, they are the object of cyber-attacks and the medium through which the cyber-attacks spreads to other organizations. Those actions are expressed, inter alia, by increasing awareness of the threats, by instituting norms, and by providing tools to improve and manage defenses against cyber incidents and minimize the potential of them materializing.

3.2 The importance of preparing for cyber crises, and basic assumptions

Most cyber incidents are handled adequately by the organization's technological response teams and do not cause significant long-term damage. However, cyber-attacks that have occurred around the world and the substantial long-term damages that they caused, have demonstrated that a different response and capabilities that are more comprehensive must be developed, beyond assimilating cyber-defense technologies and actions to contend with short-term cyber incidents. Therefore, a supplementary layer in the civilian cyberspace defense efforts is ensuring cyber preparedness for crises situations, which should help reduce the likelihood that a cyber incident

[3] Resolution of the Ministerial Committee on National Security Affairs (the Security Cabinet), of June 15, 2016.

[4] Government Resolution 3611 of August 7, 2011 on the subject of "Advancing National Cyberspace Capabilities".

[5] Government Resolution 2444 of February 15, 2015 on the subject of "Advancing the National Preparedness for Cyber Security".

will evolve into a cyber crisis, and if a crisis does materialize, to help manage it effectively.

Two basic assumptions underly the concept, which emphasize the importance of carrying out cyber preparedness while considering the circumstances prevailing in cyberspace and in the physical space:

1. A cyber crisis is liable to cause real damage and disrupt functional continuity, and to escalate to the point of a national state of emergency. For example, in December 2015, a cyber-attack was launched against the Ukrainian electric grid and disrupted the supply of electricity to hundreds of thousands of households for several hours. During another incident, in May 2017, the international cyber-attack "WannaCry" compromised the computer network of the National Health Service in Great Britain. In both cases, vital cyber assets were damaged, which attested to the quantum leap in the audacity of the attackers and to the intensification of the cyber threat.

2. Emergency situations caused by a non-cyber physical trigger (for example: war, terrorist attacks, natural phenomena, etc.) increase the likelihood that a cyber crisis will erupt, since cyber-attackers redouble their efforts during emergencies[6] and simultaneaously cause for a heightened dependence on the normal functioning of vital cyber assets.[7] For example, during the confrontation between Georgia and Russia that began in August 2008, cyber-attacks were launched soon after, which paralyzed government and communications sites in Georgia and its telephone network collapsed. Another cyber-attack caused an explosion in the oil pipeline that runs through Georgia to Europe (the Baku-Tbilisi-Ceyhan pipeline, which contributes enormously to the Georgian economy). Another example was during 2014 Israel-Gaza conflict in August 2014, during which Israel was forced to contend with a cyber-attack on military and civilian targets, which intensified parallel to the expansion and deepening of the military operation.

3.3 The concept's objectives, and target audience

The National Cyber Concept derives from the understanding that the crisis preparedness and management requires a joining of forces, coordination and cooperation at the national level, and that only in this way will their objectives be achieved. Therefore, the National Cyber Concept is intended for government ministries, regulatory authorities and state cyber-security organizations, since they are leading the state's defensive efforts to contain the attacks and their ramifications, and are advising and guiding local organizations. The National Cyber Concept is also accessible and recommended for local organizations, so that they will be aided by it and familiarize themselves with the operations being performed at the national level.

[6] The attacker strives to create another arena requiring a response or, alternatively, will exploit the fact that attention is being diverted to dealing with the existing emergency. This is why a cyber crisis is likely to be triggered at the same time as the occurrence of another type of emergency.

[7] Such as cyber assets that support critical services and enable the fabric of life to continue and the continuity of the economy's vital functions.

The National Cyber Concept's objective:

1. To serve as a fundamental basis that defines the principles and modes of action on the subject of crisis preparedness and management in the civilian cyberspace.

Secondary objectives:

1.1. To create a common language and constitute a foundation for deepening the cooperation and discourse on the subject of cyber and crisis situations, between state and private parties.

1.2. To serve as a tool providing order and guidance that every organization can use in building a cyber preparedness and management plan in the event of crisis. This in order to maintain functional and business continuity, and to help organizations ascertain the extent of their organizational preparedness in this regard.

1.3. To serve as a foundation for the INCD and other parties to develop future tools on the subject of cyber preparedness and management in the event of crisis, such as procedures, methodologies, and best practices, all of which should help assimilate and implement the National Cyber Concept in the Israeli economy.

Since a cyber crisis is liable to be severely damaging to an organization's reputation, its assets, its functionality or ability to achieve its key objectives (to the point of jeopardizing its very existence), and since a wide spectrum of organizational and business aspects must be addressed during such an event, crisis preparedness and management are the responsibility of the organization's top echelon. Therefore, the National Cyber Concept was written for organizations' boards of directors and managements. The concept is also intended for the professional echelon, particularly for cyber-security and emergency prepardness managers and for those responsible for risk management, functional and business continuity.

4. MAPPING OF THE VITAL CYBER ASSETS

4.1 What requires defense

On a daily basis, there is a saturation of cyber threats and attacks on cyber assets. In most cases, the defense efforts contain the attacks and enable operations to continue. Despite this, instances when cyber-attackers succeed in their efforts, whether because they overcame the existing defense systems or exploited the human factor,[8] are not an aberrant scenario. Cases like these can develop into a cyber crisis, particularly when the attack hits vital cyber assets, which is liable to cause critical damage to routine operations and to reputation, economic damage and endanger human lives. Therefore, *a real threat of harm to a vital cyber asset, or actual damage to it, are a basis for identifying cyber crises and ascertaining their severity*.

In order to minimize the likelihood of the occurrence of a cyber crisis, and in order to formulate an adequate response that will minimize its damages and ramifications while defining and efficiently utilizing resources and capabilities, at the initial stage, every organization should map the vital cyber assets most relevant to it. These are cyber assets whose regular functions are essential in order to maintain the functional continuity of the core processes that it manages.

According to the Cyber Defense Methodology for an Organization (CDMO)[9] developed at the INCD, the defense must be commensurate with the potential damage; i.e., the investment in defending each asset should be commensurate with the level of its criticality to the organization's functions and to its objectives that it serves or were defined for it. Therefore, the majority of the investment in defense capabilities needs to focus on the vital cyber assets. From the attacker's perspective, these assets are an attractive target for cyber-attacks, and therefore, the threat posed to them is great.

4.2 Mapping vital cyber assets

At the organizational level, every organization can use the CDMO to correctly and efficiently map the vital cyber assets that it holds and rank them according to order of criticality, to assess risks to the assets and build a plan to enhance the level of cyber-security relevant to them.

At the national level,[10] which is the focus of the concept presented in this document, two main axes for mapping vital cyber assets are carried out by the INCD in a bottom-up process, and the work carried out at the National Emergency Authority ("RACHEL") and by government ministries in a top-down process:

4.2.1 Bottom-up definition of vital cyber assets: Along this axis, the examination begins at the bottom. The INCD examines the core processes in organizations, and identifies cyber assets whose normal functions are essential in order to maintain

[8] For example, by a phishing attack.

[9] The CDMO can be found on the INCD's website, https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf

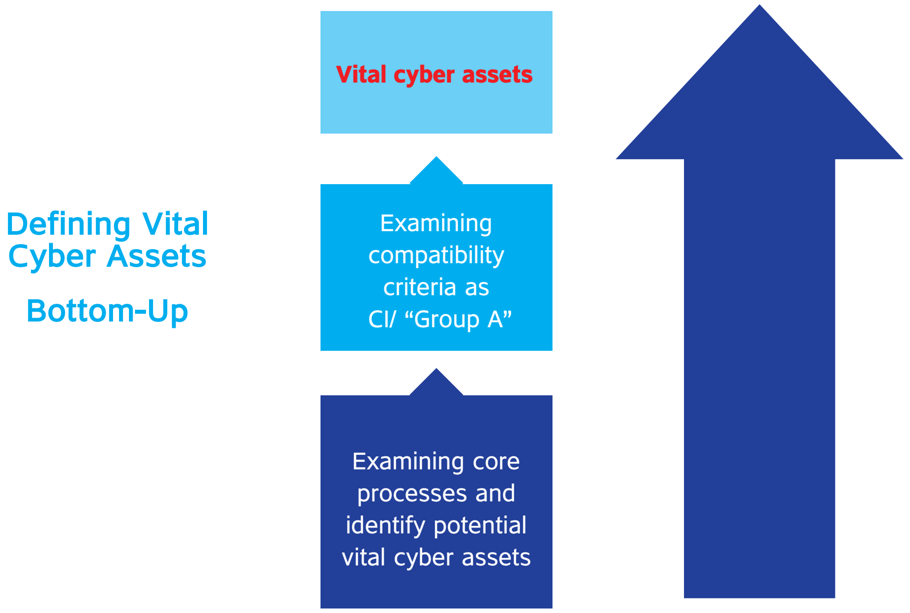
[10] The mapping of national vital cyber assets is done under the leadership of state cyber-security organizations and with the assistance of government ministries and regulatory authorities. At issue are cyber assets that are necessary for ensuring the national functional continuity and daily routine, when damage to them is liable to cause substantive damage to the State of Israel.

the continuity of core processes. Subsequently, it examines the cyber assets that were identified against criteria formulated at the INCD, that are used as a pro-active mapping mechanism to define organizations that, if hit by a cyber-attack, the damage to them is liable to cause substantial damage to the State of Israel. Cyber assets found to fulfill the criteria are defined as vital cyber assets and divided into two groups of organizations:

a. Critical infrastructure (CI) organization: an organization holding a cyber asset that fulfills the highest criteria is submitted for discussion by the steering committee for the protection of vital computerized systems, which is chaired by the director of the INCD.[11] Inter alia, its role is to ascertain which organizations should be defined as "critical" and therefore, need a high level of cyber defense. Organizations approved by the steering committee and later, also by the Knesset Internal Affairs and Environment Committee, receive guidance by virtue of law[12] directly by the CI Division in the INCD, or through a special unit of the Israel Security Agency (Shin Bet).

b. "Group A" organization: In order to build effective capabilities for increasing the level of resillance of the civilian sphere against cyber threats, the INCD takes action to define various focus groups, and provides each of them with differential guidance. The majority of the guidance resources will be allocated to a small group of organizations (hundreds of organizations) called "Group A," based on the understanding that they are holding vital cyber assets which have a major impact on key processes in the economy and a cyber-attack on them is liable to cause considerable damage.

Diagram 1:



Vital cyber assets
Examining compatibility criteria as CI/ "Group A"
Examining core processes and identify potential vital cyber assets
Defining Vital Cyber Assets
Bottom-Up

[11] This steering committee was formed as a result of Government Resolution B/84 of December 19, 2002, on the subject of "Responsibility to protect Vital Computerized Systems."

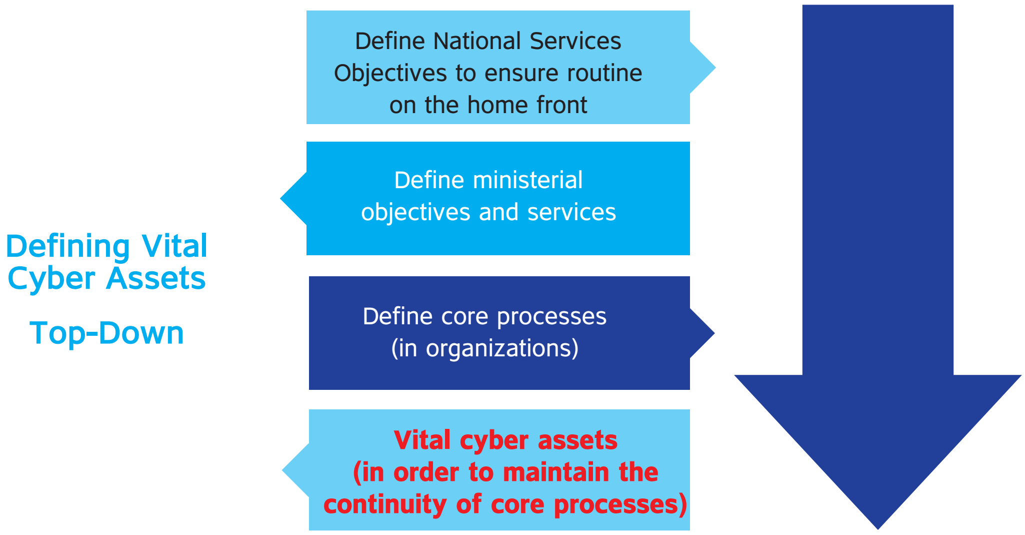
[12] Regulating Security in Public Bodies Law (Temporary Order), 5776 - 2016.

4.2.2 Top-down definition of vital cyber assets: another axis for defining national-level critical cyber assets relates to the work being done by the National Emergency Authority and government ministries in the field of functional continuity of the economy. Along this axis, the examination begins at the top, since it begins with the "National Service Objectives", which are the practical definitions of systems' services and functions that must continue even during crises, in order to ensure the national functional continuity and routine on the home front.[13]

As a derivative of the "National Service Objectives" and in order to enable their fullfilment, the National Emergency Authority works with the government ministries to define ministerial objectives and service levels, which are the practical and quantitative definitions of functional capabilities in the government ministries and in organizations under their responsibility. Capabilities that must be maintained to the extent possible, even during crises.

The achievement of the objectives and service levels defined by the government ministries is contingent upon the continuity of core processes being implemented amongst organizations, and the functional continuity of many of them depend upon cyber assets. Through use of a questionnaire that was prepared by the INCD,[14] every regulatory authority is required to work with the organizations under its responsibility in order to map and identify cyber assets, and then define which are vital cyber assets that will require to maintain a high level of cyber defense.

Diagram 2:



Defining Vital Cyber Assets

Top-Down

Define National Services Objectives to ensure routine on the home front

Define ministerial objectives and services

Define core processes (in organizations)

Vital cyber assets (in order to maintain the continuity of core processes)

[13] Such as suitable food and beverages, the provision of health services, maintaining the stability of the economic system, etc.

[14] See Appendix A.

4.2.3 Supply chain: An important stage in the process of mapping vital cyber assets and protecting them, in each of the axes described above, is examining the supply chain. The operation of many organizations depends on services that they purchase or receive from external suppliers, such as subcontractors that manufacture computer components, providers of computing services and more. Since these services may be connected to the organization's systems, they are also connected to the vital cyber assets. Consequently, every organization is required to map and identify the threats and risks contained in the systems and services of their suppliers, and to include them as part of their investment in protecting the vital cyber assets.

5. CYBER STATES OF ALERT AND PRINCIPLES FOR CHANGING THE ALERT LEVEL

5.1 General

Cyber states of alert constitute a common language reflecting the requisite degree of vigilance and preparedness to contend with the prevailing circumstances in the civilian cyberspace and in the physical space. They will be determined subject to a situational assessment, which should help develop an understanding of what is occurring based on information, facts and joint analysis, after which, the actions to be performed will be defined. A declaration of a cyber state of alert that corresponds to the reality and the magnitude of the threat, and the actions to be taken accordingly, will help reduce the likelihood of damage to vital cyber assets. Moreso, it can help minimize the development of a cyber crisis, and, if such already occurred - to minimize the damage that was caused. On the other hand, a failure to declare an appropriate state of alert will cause wide-scale damage - damage that could have been avoided or, at the very least, reduced.

5.2 Severity scheme: traffic light

As long as it has not otherwise been declared, an organization is in a state of "defense routine" and carries out routine operations and plans for crises.[15] In this situation, no disruption of the normal functioning of the organization's vital cyber assets is indicated. A substantive threat of damage to a vital cyber asset or possible disruption of its normal operations (even if it has not yet been proven that it derives from a cyber incident), reflects a possbile escalation and increases the likelihood of the occurrence of a cyber crisis. In an extreme scenario, extensive and prolonged wide-scale damage to vital cyber asset(s) causes substantial damage to core processes and to organizational business continuity.

Diagram 3:

Severity Scheme: Traffic Light

(What occurs in the organization's systems at any given time)

Stage	Description
Defense Routine	Green: no indication of disruption the functional continuity of vital cyber assets
Escalation	Yellow: substantive threat to a vital cyber asset. Functional continuity of a vital cyber asset may be compromised
	Red: damage to vital cyber asset(s) that may cause substantial malfunction in continuity of core processes
	Black: extensive and prolonged wide-scale damage to vital cyber asset(s) causes substantial damage to core processes and to the organizational functional continuity

[15] As will be explained later, in the section "Preparing for Crises."

5.3 Indicators for determining the cyber state of alert: cyberspace and the physical space

A cyber state of alert will be determined using indicators that rank the severity of the threat and the likelihood of their materialization, thus indicating what actions should be taken and what resources and tools should be used. Since emergencies caused by a non-cyber trigger (such as: war, natural phenomenon, terrorist activities, malfunction, etc.) often serve as opportunities for cyber-attackers to step up their efforts, precisely when the normal functioning of vital cyber assets become even more essential, the cyber state of alert will be determined not only by the circumstances in cyberspace, but also by the circumstances in the physical space.[16]

Two important emphases within the context of the correlation between the indicators and the states of alert:

a. The fulfillment of a particular indicator does not necessarily dictate a specific level of cyber alert, but rather, the indicators are tools used in conjunction with a situational assessment for deciding the level of alert.

b. A cyber alert might be declared even before any cyber incident occurs and without any indications of harm to vital cyber assets. This could be as a result of informational alerts or due to circumstances that increase the dependence on and importance of the normal functioning of vital cyber assets. In other words, an organization can be define in a cyber alert level A or B at the same time as it has a “green light” in the severity scheme.

Following are details about cyber states of alert and the indicators for deciding each level:

5.3.1 Cyber Routine

This is the default situation, when circumstances in cyberspace and in the physical space show no indications of a disruption of the normal functioning of vital cyber assets, or any need to raise defense. Under these circumstances, indicators for higher levels of alert have not been fulfilled.

Indicators in cyberspace: either no visible cyber incidents occurred, or cyber incidents have occurred, but without disrupting vital cyber assets.

Indictors in physical space: general alerts.

5.3.2 Cyber alert level A

Cyber alert level A will be determined following a situational assessment,[17] and provided that at least one of the following indicators has been met:

Indictors in cyberspace: a cyber incident has occurred that indicates possible disruption to the normal functioning of a vital cyber asset; the receipt of an informational alert; an annual cyber-attack has occurred (such as “OpIsrael”)[18]; an cyber event has occurred abroad that has not yet spread to Israel (such as “WannaCry”); a cyber incident attributed to Israel.

Indictors in physical space: an operational/technical malfunction in a vital cyber asset and/or at the site where it is located; warning of a wide-scale security event or the occurrence of an aberrant security event (such as: an escalation in missile launches towards Israel, or an attack occurred that is attributed to Israel); an upgrade

[16] As explained in section 3.2.

[17] See Appendix B for more information about cyber situational assessment.

[18] Annual coordinated cyber-attack against Israel, initially launched in April 2013.

in the level of alert by the IDF; an irregular event has occurred that is liable to impact cyberspace.

5.3.3 Cyber alert level B

Cyber alert level B will be determined following a situational assessment, and provided that at least one of the following indictors has been met:

Indictors in cyberspace: immanent warning of a cyber-attack; damage to vital cyber asset(s) and, as a result, potential real disruption of the continuity of a core process.

Indictors in physical space: physical damage to services that are vital to the economy (such as: power outage, disruption of health services); an extensive security event has occurred (such as a limited military operation).

5.3.4 Cyber alert level C

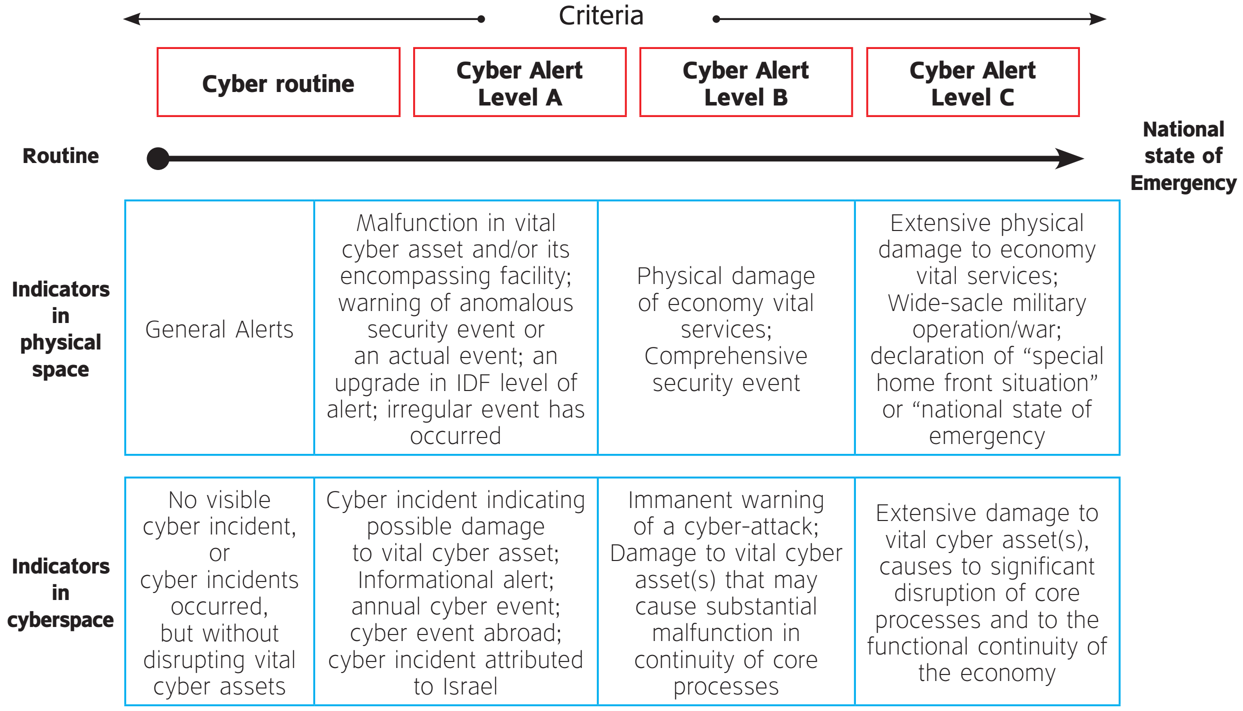
Cyber alert level C is the highest level of cyber alert, such that the circumstances that prompted the declaration of this state of alert are liable to escalate to the point of a national state of emergency. Cyber alert level C will be determined following a situational assessment, and provided that at least one of the following indicators has been met:

Indicators in cyberspace: extensive and/or persisting damage to vital cyber asset(s), leading to significant disruption of core processes and to the functional continuity of the economy (such as damage that crosses sectors).

Indicators in physical space: extensive and/or persisting physical damage to services that are vital to the economy; war or a wide-scale military operation; the declaration of a "special home front situation"/"civilian emergency event."

Diagram 4:

Cyber states of alert



	Cyber routine	Cyber Alert Level A	Cyber Alert Level B	Cyber Alert Level C
Indicators in physical space	General Alerts	Malfunction in vital cyber asset and/or its encompassing facility; warning of anomalous security event or an actual event; an upgrade in IDF level of alert; irregular event has occurred	Physical damage of economy vital services; Comprehensive security event	Extensive physical damage to economy vital services; Wide-sacle military operation/war; declaration of "special home front situation" or "national state of emergency
Indicators in cyberspace	No visible cyber incident, or cyber incidents occurred, but without disrupting vital cyber assets	Cyber incident indicating possible damage to vital cyber asset; Informational alert; annual cyber event; cyber event abroad; cyber incident attributed to Israel	Immanent warning of a cyber-attack; Damage to vital cyber asset(s) that may cause substantial malfunction in continuity of core processes	Extensive damage to vital cyber asset(s), causes to significant disruption of core processes and to the functional continuity of the economy

5.4 Principles for changing the cyber state of alert

During each state of alert, each organization will conduct a situational assessment, examine the indicators in cyberspace and in physical space and will then ascertain whether there is a need to change the state of alert.

5.4.1 Upgrading the level of the cyber alert: upgrading the level of the cyber alert derives from a substantive possibility of an escalation in the prevailing circumstances, which mandates that actions should be taken that have not yet been taken, or moderately increasing the intensity and scope of the actions already taken, to the extent possible. The purpose of these actions is to prevent further exacerbation or at least to minimize the damage that will be caused. The level of alert should be upgraded gradually, according to the indicators, but not in all situations. For example, in an extreme situation, a cyber alert level C might be declared before another alert level has been defined.

5.4.2 Downgrading the level of the cyber alert: A level of alert will be downgraded if the indicatros that led to the determination of the level of alert are no longer being met. The level of alert is downgraded gradually; i.e., by one category each time, until the cyber routine is restored.

5.5 Tiers for declaring a cyber state of alert

In light of the methodology presented above, there are three main tiers for declaring a state of alert in civil cyberspace: the national level, the sectoral level[19] and at the organizational level. In light of the considerable importance of sharing information, and considering the rapidity at which cyber incidents occur, it is essential for every organization that changes its state of alert to update all relevant parties in this regard, including the INCD, the regulatory authorities and other subordinate organizations (if any). For the most part, the updating is done covertly, which enables "covert defense"; i.e., responding to the cyber incident while carefully concealing the defensive actions in order to contain the attack and learn the attacker's methods and activities.

a. *At the national level*, the Director-General of the INCD will declare the cyber state of alert, as the professional responsible for defending civilian cyberspace, or his/her delegate. This cyber alert is declared following a threat or circumstances that are liable to escalate to the point of a national state of emergency. A national-level cyber alert is binding upon all sectors in the economy. A sector can define a higher, but not a lower, level of cyber alert for itself than that defined at the national level.

Since sectors and organizations may be affected differently by cyber incidents at any given point in time, and reach different conclusions after a situational assessment, there are two more tiers, besides the national tier, for defining a cyber state of alert, which reflect sectoriality and possible differentiality:

[19] Sector: all organizations operating in a professional field of a government ministry and under its regulatory responsibility (from Government Resolution 2443 of February 15, 2015, on the subject of "Advancing National Regulation and Government Leadership in Cyber Defense").

b. *At the sectoral level*, the director-general of the relevant government ministry/regulatory authority, or his/her delegate, will declare the cyber state of alert, in coordination with the INCD or according to its recommendation. The declaration is binding upon all organizations under that sector's responsibility[20] or, alternatively, on defined specific organizations. The declaration of a cyber state of alert in a particular sector is not binding upon other sectors, but it indicates that circumstances exist in cyberspace that they should address.

c. *At the organizational level*, the CEO of the organization or his/her delegate will declare a cyber state of alert, in coordination with the sectoral cyber unit[21] and/or the regulatory authority, or according to their recommendations/guidance. An organization can define a higher, but not a lower, level of cyber alert for itself than that defined in the sector to which it belongs.

Diagram 5:

Principles for Changing Cyber Alert Levels and Tiers

Cyber Alert Levels	Organizational level	Sectoral level	National level	Criteria for downgrade in cyber alert levels
C	The organization, in coordination with the sectoral cyber unit/ regulator, or in light of their recommendation	The governmental ministry or the regulator, in coordination with the INCD or in light of its recommendation	INCD	The economy's functional continuity has been restored
B	The organization, in coordination with the sectoral cyber unit/ regulator, or in light of their recommendation	The governmental ministry or the regulator, in coordination with the INCD or in light of its recommendation	INCD	Removal of the threat to functional continuity and core processes. General threat levels
A	The organization, in coordination with the sectoral cyber unit/ regulator, or in light of their recommendation	The governmental ministry or the regulator, in coordination with the INCD or in light of its recommendation	INCD	Indicators for declaring cyber alert level A are no longer met
Cyber Routine				

[20] Exceptions are CI organizations listed in the addendum to the Regulating Security in Public Bodies Law, which receive direct guidance in relation to cyber aspects by the INCD or by a designated unit in the Israel Security Agency.

[21] A sectoral cyber unit operates subordinate to its relevant government ministry, and is a unit providing professional cyber-security guidance to organizations over which that government ministry has regulatory authorities. The unit is professionally guided by the INCD (from Government Resolution 2443 of February 15, 2015, on the subject of "Advancing National Regulation and Government Leadership in Cyber Defense").

6. PREPARING FOR CRISES: TOOLBOX (TOP 5)

Considering each of the cyber states of alert described above, every organization should institute actions that will help reduce the likelihood that a cyber crisis will develop, or if it already occurred, to manage it in a way that will reduce its damages and repercussions to the extent possible. These actions during cyber routine, are being carried out sometimes on short notice, either in a limited manner or are not being carried out at all. Therefore, the higher the level of alert, the more that higher-intensity and wider-scale actions will be necessary.[22]

In order to ensure that organizations will be able to carry out the required actions while managing the crisis, organizations must prepare for them when still in cyber routine. Actions that have not been prepared beforehand cannot be performed during a crisis, or it might be possible to perform them partially, at a delay and not optimally. To avoid such a situation, a significant stage in preparing for cyber crises is building a toolbox in advance.

Since a cyber crisis is not only a technological issue, when building the toolbox it is important to emphasize not only technological resources, but also focus on how to improve the skills and know-how of the human resources. All these are "power multipliers" for the organization. Some of the components are also used during routine times (such as assimilating technological systems, as well as training and exercises), while other components are operated only in preparation for an impending crisis, or while it is actually occurring (such as activating the crisis management team).

Every organization is responsible for preparing its own toolbox, while taking into account the risk assessment that it performed, the threat scenario it may face in cyberspace[23] and considering its needs and resources. The composition of the toolbox will also be determined according to the objectives and service levels prescribed by the government ministries, within the context of assuming their share of the state's responsibility for ensuring the proper achievement of the "National Service Objectives".[24] Consequently, the regulatory authorities play a very important role in defining the level of functional continuity that is required of the organizations under their responsibility. All organizations will build their toolboxes in light of the defined cyber alert level, will allocate a designated budget for it and another readily-available budget for emergencies, to be incorporated in their work plans.

When building the toolbox, it is recommended to take five power multipliers into account: *professional know-how; manpower; technologies and means; assistance from outside sources; training and exercises*. Since the National Cyber Concept is intended both for state organizations and institutions, and for public and private organizations, every organization can use the examples given below and customize its toolbox according to its needs.

[22] See section 7 for more information.

[23] The threat scenario is based on an assessment and defines the plausible playbook for hostile activity and its modus operandum. Organizations can receive assistance from external professionals in formulating the threat scenario.

[24] As explained in section 4.2.2.

6.1 Professional know-how

a. The concept presented in this document should be assimilated in organizations as a framework for a common language and for deepening the cooperation and discourse, and as a tool for building a cyber crisis preparedness and management plan. This plan can be a chapter in the organization's emergency plan,[25] or a separate document, and it is recommended that the plan should be written with the professional assistance of the INCD and/or the regulatory/guiding authority, and should be approved by the organization's management. It is advisable to validate and update the plan annually, and to review it when a state of alert is upgraded.

b. The Cyber Defense Methodology for an Organization (CDMO), which was developed by the INCD in order to mitigate the cyber risks of organizations, should be assimilated. The CDMO defines an orderly methodology that every organization can use to learn about the risks that are relevant to it, to formulate a defense and risk-mitigation plan accordingly. The CDMO, and additional professional publications addressing cyber defense can be found on the INCD's website.[26]

c. Organizations can avail themselves of doctrines, procedures and best practices, which were written by the INCD, the relevant regulatory authority or international cyber experts (such as standard institutions), that focus on cyber crisis preparedness and management.[27]

6.2 Manpower

The human factor is an integral part of cyber crisis preparedness and management, and crises have an impact on the composition of the manpower, due to the need to work more intensively and with more manpower than during cyber routine, or due to employee absences.[28] Therefore, organizations should take into account the deployment of manpower during crises, define essential functionaries and spheres of responsibility, build a plan to back-up and reinforce essential manpower at all echelons, and examine work modes and methods for functioning with limited manpower.

a. Assembling a crisis preparedness and management team: Since the organization's management assumes the overarching responsibility for crisis preparedness, and it will be managing the crisis if it materializes, it is recommended that the organization's CEO or deputy CEO should head the team. A cyber crisis is not only a technological matter, and therefore, in addition to the chief information security officer (CISO), it is advisable that the crisis preparedness and management team include senior management members, who have been highly familiar with the organization's work processes and whose backgrounds are in various disciplines (such as: the COO, CFO, legal counsel,

[25] Business continuity plan - BCP.

[26] https://www.gov.il/en/Departments/Policies/cyber_security_methodology_for_organizations

[27] For more information on the subject of cyber-security standards and regulations: https://www.gov.il/he/Departments/legalInfo/regulation

[28] This is relevant when a cyber crisis erupts at the same time as a crisis in physical space.

logistics manager, spokesman, security officer). This team is responsible for preparedness during routine times while, during a crisis, it is responsible for managing all aspects of the crisis: compiling a situation overview to assess the situation,[29] announcing the state of alert and changing the level of alert, dictating relevant actions following the state of alert, working with sources inside and outside the organization and, finally, recovery. The team will then veryify that the organization has returned to cyber routine, will run an analysis of lessons learned and make sure to assimilate them.[30]

b. Forming a CSIRT:[31] a professional team whose mission is to detect, prevent, contend with and handle cyber incidents and the recovery from damages. This team includes cyber and information security professionals and IT professionals comprising employees of the organization or outside experts that the organization chooses. During a crisis, the CSIRT reports directly to the crisis preparedness and management team and works in consultation and coordination with representatives of other units inside and outside the organization.

c. Manpower deployment during emergencies: The organization should map its manpower strength, its capabilities and qualifications, and build a picture of the gaps in manpower and their skills that it needs to learnt, in order to ensure functional continuity also during a crisis. This process will help organizations create emergency teams; i.e., during a crisis, the roles of some employees will differ from their roles in routine times. In addition, it will help identify specific roles that need reinforcement (internal disbursement of manpower or assistance from external organizational sources). To achieve optimal performance, the employees should be trained and receive exercises in this regard during routine times.

d. Defining the organization as a "critical enterprise":[32] Obtaining certification as a "critical enterprise" enables the organization to use, inter alia, two important tools for contending with crises in the context of manpower: 1) "round-the-clock on-duty" status for critical personnel to ensure the organization's functional continuity (such as cyber security personnel). An employee in the military reserves, who was authorized for "round-the-clock on-duty" status, will fulfill his/her service during an emergency at the critical enterprise where he/she works, and will not be called for military service; 2) identifying, defining and approving "outside recruits" - professionals who are not employees of the organization, who are called to work there during a crisis as a source of reinforcements. It is important to establish work relations with outside recruits during routine times.[33]

e. Assembling a reserve of cyber experts: an organization can assemble a reserve of volunteers who are experts in a variety of cyber disciplines,

[29] For more information, see Appendix B.

[30] For more information, see the section "Cyber Crisis Management."

[31] Computer Security Incident Response Team; also called CERT - Computer Emergency Response Team.

[32] Enterprise (organization) or a portion thereof, which operates or may be operated for purposes of state defense, public security and for the provision of vital services to the economy, and which must continue functioning also during crises. Defining an organization as a "critical enterprise" is subject to approval by a committee appointed by the Minister of Labor, Social Affairs and Social Services (Emergency Labor Service Law, 5727-1967).

[33] Additional information on these topics may be found on the Emergency Manpower Authority's page on the website of Israel Ministry of Labor, Social Affairs and Social Services.

who will assist the organization in routine times and during a crisis, both as a think-tank and brainstorming team and for the provision of technological and managerial solutions.

6.3 Technologies and resources

Organizations should equip themselves with technologies and resources to help them enhance the level of cyber defense, reinforce their capabilities in detecting and responding to cyber attacks, managing crises, and all while simultaneously maintaining functional business continuity processes.

a. Assimilating systems: 1. security technologies (identification, encryption, preventing hostile code, etc.); 2. recording and monitoring systems in order to detect cyber incidents (which events will be logged with defined periods of time, and assimilating SIEM system); 3. technologies focusing on detecting, deflecting and investigating attackers (such as honeypot and sandbox); 4. data backup and recovery technologies to ensure rapid recovery; 5. crisis management and documentation systems. These technological systems must be updated regularly, or according to the guidance from the regulatory authority/ guidance unit. Additionally, its beneficial to consider the possibility of connecting to the "Cyber Net" system of the Israel's National CERT, which enables information-sharing to help contend with cyber threats and cyber incidents.

b. Physical resources: establish an alternative, separate disaster recovery site (DR) that is physically remote from the organziation's main site and complies with a high standard of security, in a manner that reduces the likelihood that both sites will be attacked simultaneously, and enables back-up and restoration of information. It is crucial to assimilate procedures and controls for entering the organization's facilities, in order to prevent a cyber-attack through physical means.

c. Logistics resources: equipping the organization with logistic and administrative means to assist those working during a crisis (remote work, food, supplies, transportation, etc.); equipping with physical means of protection that are needed during non-cyber emergencies; periodic inspections of the working order of the infrastructure and means.

6.4 External sources

Many professionals can provide cyber assistance to organizationsin order to help improve preparedness and during crises.

a. Public sector: using the professional tools provided by the INCD and the regulatory authorities (such as: professional know-how, responses to cyber incidents, training, instruction, exercises, audits, and more).

b. Private sector: if an organization chooses to avail itself of the services of private companies (such as: risk-management advisors, response to cyber incidents and cyber crisis management, insurance, etc.), it is essential that an undertaking be added to the SLAs signed with them that the response will also be given during a crisis. It is important that such outside service-providers are familiar with the organization's cyber crisis prepardness plan and, if possible, they should participate in related exercises and be updated when an irregular event occurs. Additionally, organizations can use know-how and tools available at corresponding organizations around the world.[34]

[34] Such as the information sharing and analysis center of the FS-ISAC, the members of which include global financial organizations.

c. Cooperation agreements: organization can take action to create written or oral agreements with other relevant organizations (such as from the same sector), for mutual assistance and cyber cooperation in routine times.

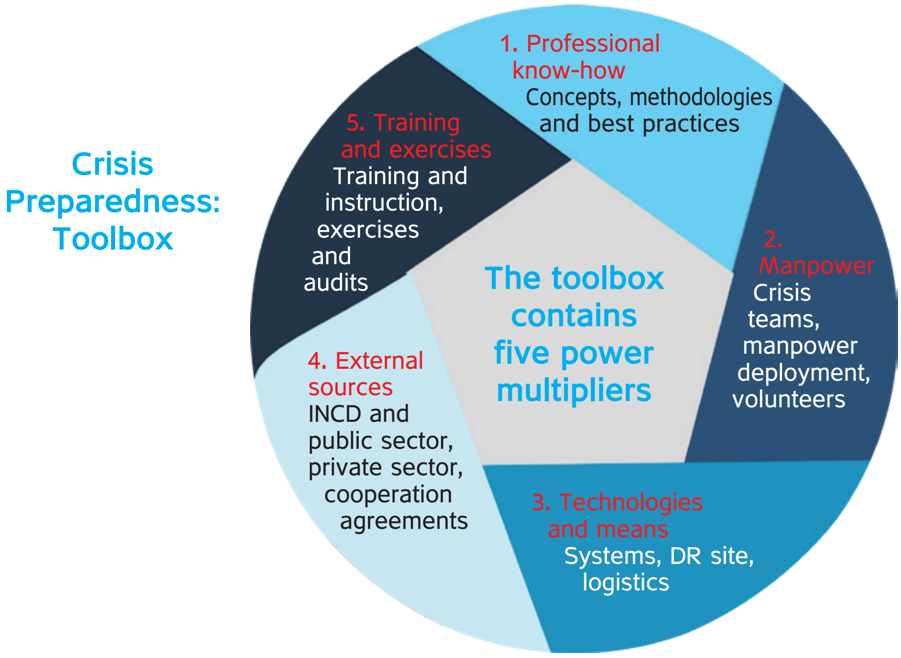
6.5 Training and exercises

Many cyber-attackers succeed in overcoming defense mechanisms by using social engineering, exploiting the human factor, such as through phishing (the attacker impersonates another party). On the other hand when cyber incidents occur, the human factor is an integral component of the response and therefore, training and exercises are very important components of preparing for crises and for enhancing an organization's resilience.

a. Training and instruction: These should be offered to personnel in the organization in order to increase awareness and create an organizational culture relating to cyber threats, and also in order to build and maintain qualifications. Training ensures that employees will perform their roles optimally both in routine times and during emergencies (particularly employees who perform a different role during emergencies than they do normally). At the management echelon, it is important to include training and instruction to strengthen soft skills, such as decision-making capabilities, teamwork and communications skills.

b. Exercises and audits: These can vary in scope (individually, organization-wide, sector-wide) and methods (theoretical and operational exercises, simulations, overt/covert audits and penatration tests). The exercises and audits should be part of the annual work plan and encompass the largest number of functionaries as possible, including at the management level and the crisis management team, and it should be carried out in conjunction with outside sources with whom the organization has interactions. The exercises and audits should be challenging and reflect the organization's cyber crisis preparedness and management plan, and after completed, the insights gleaned should be used to draw conclusions and make adjustments in the plan.

Diagram 6:


Crisis Preparedness: Toolbox
1. Professional know-how
Concepts, methodologies and best practices
2. Manpower
Crisis teams, manpower deployment, volunteers
3. Technologies and means
Systems, DR site, logistics
4. External sources
INCD and public sector, private sector, cooperation agreements
5. Training and exercises
Training and instruction, exercises and audits
The toolbox contains five power multipliers

As part of the toolbox, a questionnaire is attached in Appendix C, which is intended to serve as a work tool for assessing the organization's level of preparedness for cyber crises, and which proposes insights about topics needing improvement.

7. CYBER CRISIS MANAGEMENT

7.1 The life-cycle of a cyber crisis

Every cyber crisis has its own unique life-cycle. Some cyber crises manifest themselves as sudden outbursts with immediately apparent ramifications, while other crises are built gradually (but even if a gradual escalation is observed, it is still possible that a crisis will erupt later). The initial information can come from various sources: monitoring systems, indications detected in data or in business information, reporting from an internal source, or an update provided by an outside source (such as the INCD or a regulatory authority/guidance unit). Considering the high speed at which a cyber crisis can erupt and the risk that it might spread to additional organizations and sectors, any employee who detects a suspected cyber incident, or who receives a report in this regard, must immediately notify all relevant personnel both inside and outside the organization.

The life-cycle of a cyber crisis can be described as a process with multiple stages:

Detection: discovery of an irregular occurrence, in terms of its effects on the organization's vital cyber assets and core processes (threat or actual disruption), and formulation of the required type of response as rapidly as possible.

Analysis: comprehensive and in-depth clarification of the nature of the occurrence and verifying that there are no further breaches, and analyzing its effect on the organization's functionality, beyond the technological aspects.

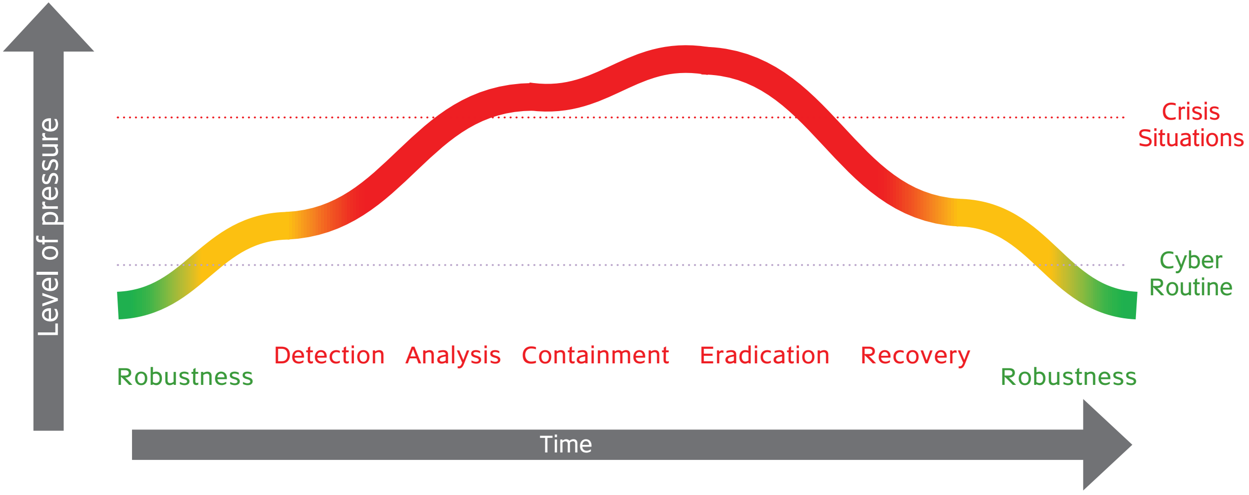
Containment: blocking the attack (gaining initial control) and its spread to other cyber assets, and containing the damage that it is causing (business continuity, reputation, economic damage). Containment is according to the organization's crisis management plan.

Eradication: neutralizing the attack components while attempting to reverse or minimize the damage already caused, to the extent possible.

Recovery (restoration): controlled return to normal operations, announcing the end of the crisis (back to cyber routine), carrying out an inquiry and drawing lessons learned, and defining measures for implementation.[35]

Diagram 7:

The life-cycle of a cyber crisis



[35] The Diagram taken from ENISA's website, the European Union Agency for Network and Security Information.

7.2 The concept of cyber crisis management: crisis-management team

When managing a cyber crisis, several key targets (objectives) must be defined:

- To minimize the functional, business-economic and reputational damage.
- To protect the vital cyber assets and sensitive information.
- To continue providing optimal services even during the crisis, particularly critical services.
- To boost stakeholders' confidence through proven capabilities in contending well with crises.
- To conclude the handling of the causes of the crisis as rapidly as possible, to recover and return to routine.

The management of a cyber crisis must address threats and challenges on two phases:

a. Contending with the causes of the crisis: the technological aspects relating to the cyber-attack and their direct impact on the cyber assets (led by the technological response team).

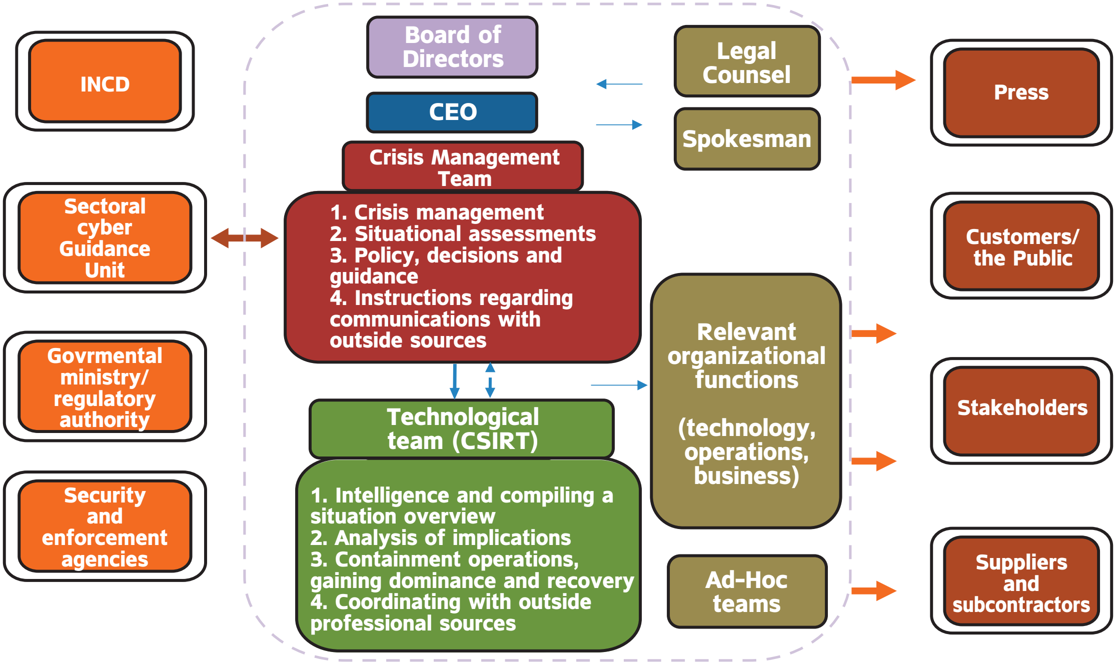
b. Contending with the ramifications of the crisis: unlike a cyber incident, a cyber crisis requires attention beyond the technological aspects, since it has implications both inside and outside the organization, such as the organization's functional continuity, business-economic implications and reputational implications.

Contending on both of these levels requires different tools, and it is under the responsibility of different organizational personnel. However, synchronized handling on both levels is exceedingly important, since there is linkage between them, and decisions at one level may affect the other level. Therefore, and due to the grave ramifications of a cyber crisis on the organization's reputation, its assets, its functioning and/or capabilities of achieving its key objectives, a cyber crisis should be managed by a *crisis-management team* comprised of the organization's senior management echelon.[36] This team guides and directs the work of the other relevant personnel in the organization (inter alia, the technological response team), and manages the communications with the outside stakeholders, who are very important during a crisis.

[36] As explained in section 6.2.

Diagram 8:

Cyber Crisis Management Concept



INCD

Sectoral cyber Guidance Unit

Govrmental ministry/ regulatory authority

Security and enforcement agencies

Board of Directors

CEO

Crisis Management Team

1. Crisis management
2. Situational assessments
3. Policy, decisions and guidance
4. Instructions regarding communications with outside sources

Technological team (CSIRT)

1. Intelligence and compiling a situation overview
2. Analysis of implications
3. Containment operations, gaining dominance and recovery
4. Coordinating with outside professional sources

Legal Counsel

Spokesman

Relevant organizational functions

(technology, operations, business)

Ad-Hoc teams

Press

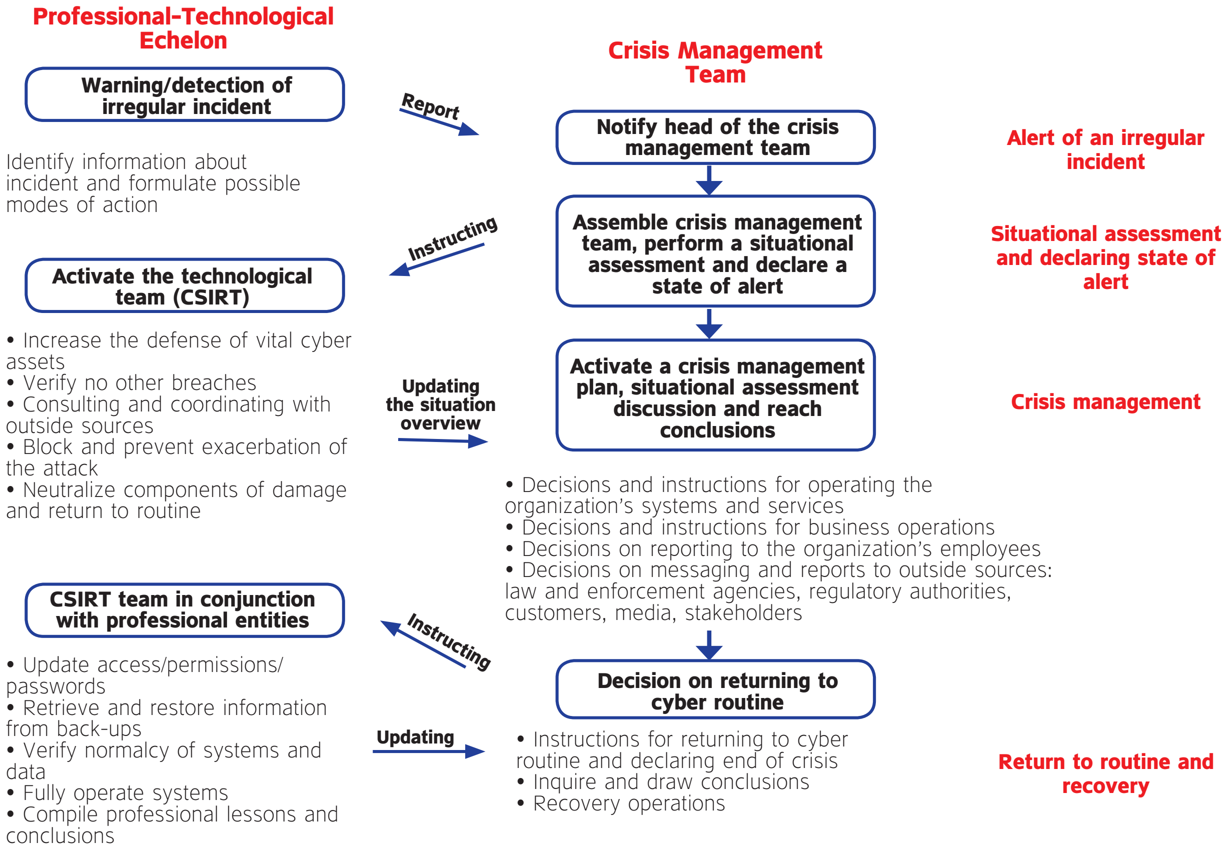
Customers/ the Public

Stakeholders

Suppliers and subcontractors

When assembling all of the components described above, the overall flow of cyber crisis management looks like this:

Diagram 9:



Professional-Technological Echelon

Crisis Management Team

Warning/detection of irregular incident

Identify information about incident and formulate possible modes of action

Report

Notify head of the crisis management team

Alert of an irregular incident

Instructing

Activate the technological team (CSIRT)

- Increase the defense of vital cyber assets
- Verify no other breaches
- Consulting and coordinating with outside sources
- Block and prevent exacerbation of the attack
- Neutralize components of damage and return to routine

Assemble crisis management team, perform a situational assessment and declare a state of alert

Situational assessment and declaring state of alert

Updating the situation overview

Activate a crisis management plan, situational assessment discussion and reach conclusions

Crisis management

- Decisions and instructions for operating the organization's systems and services
- Decisions and instructions for business operations
- Decisions on reporting to the organization's employees
- Decisions on messaging and reports to outside sources: law and enforcement agencies, regulatory authorities, customers, media, stakeholders

CSIRT team in conjunction with professional entities

Instructing

- Update access/permissions/ passwords
- Retrieve and restore information from back-ups
- Verify normalcy of systems and data
- Fully operate systems
- Compile professional lessons and conclusions

Updating

Decision on returning to cyber routine

- Instructions for returning to cyber routine and declaring end of crisis
- Inquire and draw conclusions
- Recovery operations

Return to routine and recovery

7.3 Operations during management of a cyber crisis

This section specifies actions to be carrired out during cyber crisis management. For the reader's convenience, the actions are divided according to cyber states of alert. This does not mean that the declaration of a state of alert necessarily dictates the implementation of specific actions, but rather, that the states of alert help reach decisions about the appropriate actions. Therefore, in a given cyber state of alert, organizations will perform different actions, considering the danger posed to them, the situational assessment and taking into account the tools and resources available to them, or according to the regulatory authority's guidance.[37] Since the National Cyber Concept is intended for both state organizations and institutions, and for public and private organizations, every organization can use the examples specified below to make necessary adjustments. As explained in the previous section, actions not prepared ahead of time cannot be carried out during a crisis, or may be able to be carried out partially and not optimally. Before reaching a decision about an action, possible implications must be taken into account.[38]

Following are details about possible actions in each of the cyber states of alert, segmented by intra-organizational and extra-organizational actions:[39]

7.3.1 Cyber routine

During cyber routine, apart from actions to ensure routine operations under cyber threats and to contend with specific cyber incidents, the organization prepares itself for the actions that it will take during a crisis. In other words, the organization carries out routine operations, while building capabilities and raising qualifications, and maintains flexibility in preparation of transitioning to a higher cyber state of alert, as specified in the previous section discussing the toolbox.

7.3.2 Cyber alert level A

Possible actions during cyber alert level A:

Intra-organizational: Increasing alertness; updating all relevant personnel inside the organization about the heightened alert to increase availability;[40] disbursing and/or reinforcing manpower to ensure a concentrated effort; manning/reinforcing the operations control center; ongoing situational assessments; updating the situation overview and intelligence efforts; preparing press releases (rough drafts); reviewing the cyber crisis management plan and ensuring readiness to transition to a higher state of alert; performing necessary operations in computerized systems (such as: checking operability, security updates, increasing the monitoring activities, backups and more);[41] performing necessary actions relating to

[37] The guidance from the regulatory authority/guidance unit needs to be proportional, and take into account the organization's capabilities and resources and the costs involved in carrying out the actions.

[38] For example, the way that the organization chooses to publicize a cyber incident or crisis, how it contends with ransomware that tries to extort payment in exchange for restoring access, the effects on corresponding organizations and on stakeholders, the performance of actions to remove the malware, whether overtly or covertly to the attacker, etc.

[39] It is important to document the actions taken when managing the crisis, inter alia, for the purpose of conducting aninquiry and drawing out lessons learned, as specified later in this section.

[40] Secrecy must be maintained when updating internal and external parties about cyber incidents, for covert defense (low-profile activities)

[41] For more information and recommendations about operations on computerized systems, assistance may be received from the regulatory authority/guidance unit and from INCD, by contacting the National CERT (*9344).

physical security (such as: increasing alertness to irregular events in the organization and immediate reporting, tightening the procedures for entering the organization and inspecting the security means).

Extra-organizational: Updating the regulatory authority/guidance unit, INCD, partners and all relevant parties regarding the cyber state of alert and the cyber situation overview, for the purpose sharing know-how and receiving guidance and recommendations for action; issuing guidance measures to parties directed by the organization; collecting information from relevant inside and outside sources; updating and checking communications with service-providers.

7.3.3 Cyber alert level B

In a Cyber alert level B, all of the actions that the organization performed in a level A alert will be carried out, as well as:

Intra-organizational: Activating and reinforcing relevant professional teams (such as technological response teams and crisis-management team); fully manning the operations control center and working according to organizational schedule; readiness to activate the emergency manpower deployment plan; activities by the organization spokesman; performing necessary operations in computerized systems (such as: stopping the entry of files, ascertaining the need to sever nonessential links with tangential systems, reducing activities to a minimum, locating components that have been attacked, isolating the segment where the attack was detected, blocking the attack, verifying that there are no additional breaches, documentation); distributing means of protection; increasing the readiness to move to an alternative facility and checking the systems there (relevant when the escalation relates to a physical emergency trigger); performing necessary actions relating to physical security (such as: periodic patrols, strengthening security and limiting entry of visitors and only with accompaniment); reducing nonessential actions.

Extra-organizational: activating engagements with outside professional sources for the receipt of assistance (such as: cyber and information security companies, and crisis management); activating signed cooperation agreements with corresponding organizations; issuing an alert to "outside recruits" regarding the increased need of availability; activating the cyber experts reserve.

7.3.4 Cyber alert leverl C

In a cyber alert level C, the actions that the organization performed in a cyber alert level B will be carried out, as well as:

Intra-organizational: activating the emergency manpower deployment plan; activating the "round-the-clock on-duty" protocol (in organizations approved as "critical enterprises"); manning an alternative facility; performing necessary operations in computerized systems (such as severing all external links to the system); performing necessary operations relating to physical security (such as: prohibiting entry of visitors).

Extra-organizational: working according to the "National Schedule"; activating outside recruits.

Diagram 10:

Possible actions based on each cyber alert level (example)

Cyber Alert Level A		Cyber Alert Level B		Cyber Alert Level C	
Update all relevant parties	disbursing and/or reinforce manpower	Activate intra-organizational professional teams	Full manning of the organizational operations control center	Work according to the national schedule	Activate the emergency manpower deployment plan
Reinforce the organizational operations control center	Perform ongoing situational assessments	Work according to organizational schedule	Readiness to activate the emergency manpower deployment plan	Activate "round-the-clock on-duty" protocol	Activate outside recruits
Update the situation overview and the intelligence effort	Prepare press releases to the media (rough drafts)	Spokesman activities	Logistics	Man the alternative facility	Logistics
Review and work according to the cyber crisis preparedness plan	Verify readiness to transition to a higher state of alert	Activate engagements with service-providers	Activate cooperation agreements with corresponding organizations	Perform operations in computerized systems	Perform actions to enhance the physical security
Perform operations in computerized systems	Perform actions to enhance the physical security	Perform operations in computerized systems	Perform actions to enhance the physical security		

7.3.5 Recovery: returning to cyber routine

The organization's CEO or his/her delegate (such as the head of the crisis management team) will declare the return to cyber routine. Upon the declaration of the return to cyber routine,[42] all relevant parties inside and outside the organization should be updated of such. The organization should define recovery targets,[43] assess the damages caused and take action to minimize them, and draw conclusions as soon as possible in order to improve the quality of any future response to a crisis. It is important to discuss, inter alia, the following issues:

a. Chronological review of the incidents and actions taken, as of the decision to upgrade the cyber alert level and until the return to cyber routine.

b. Evaluate the organization's conduct and the effectiveness of actions taken in response to incidents in all fields (technological, managerial, logistics, spokesman, etc.), including the issue of obtaining assistance from, and cooperating with outside sources.

c. Evaluate the effectiveness of the preparations carried out during routine times ("the toolbox").

d. Identify issues needing improvement and retention, and assess future needs. Formulate lessons and conclusions, assimilate and disseminate them to stakeholders inside and outside the organization.

e. Validate the cyber crisis prepardeness plan.

[42] According to the principles for downgrading a level of alert, as specified in section 5.4.

[43] For example: returning to full business operations within a particular timeframe.

8. APPENDICES

Appendix A: questionnaire for mapping vital cyber assets

1. As part of the preparations for maintaining the functional continuity of the economy during an emergency, government ministries have defined service objectives and service levels. The process is being led by the National Emergency Authority, in conjunction with the government ministries.

2. As part of the mapping process, it is crucial to identify cyber assets (computerized systems, infrastructures, communications systems, servers, controllers, etc.) that support the core processes, in order to obtain a comprehensive in-depth picture in this regard and to define them as vital cyber assets that need a higher level of cyber security.

3. The short questionnaire below, which is based on the service objectives defined in your organization, will assist in mapping any vital cyber assets whereby harm to them will cause long-term damage.

4. It is advisable to carry out the mapping process in collaboration with the guidance division at the INCD, and with the sectoral cyber units or the relevant regulatory authority.

Task no.	Ministerial objectives	Does the service ojectives require work with computerized systems?	If it does, which system(s) support(s) the service objectives?	During what timeframe can the service objectives continue functioning without computerized systems?	Can the routine workflow be restored by using with alternative systems?	Will the level of service be impacted due to the leaking or theft of information from computerized systems?	Will the level of service be impacted due to a shutdown of any computerized systems?	Will the level of service be impacted due to data disruption in any computerized systems?
1	Please specify	No/ Yes, with minor to moderate dependence/ Yes, with considerable dependence	Please specify	Incapable/ Up to one week/ More than one week	No/ Yes, within 12 hours/ Yes, within 12-24 hours/ Yes, within 1-3 days/ Yes, after more than 3 days	No impact/ Minor to moderate impact/ Major impact	No impact/ Minor to moderate impact/ Major impact	No impact/ Minor to moderate impact/ Major impact
2								
3								
4								
5								

Appendix B: cyber situational assessment discussion

The purpose of a cyber situational assessment is to help understand the significance of recent occurences, based on information, facts and collaborative thinking and, subsequently, defining actions to be taken. The situational assessment should be spearheaded by the senior authority in the organization, or the officer authorized for this purpose, at a prescheduled time (such as weekly) or depending upon the circumstances, with the participation of the senior management echelon (usually the crisis prepardeness and management team), and other relevant professionals. The discussion itself should be brief and purposeful.

The format of the discussion of the situational assessment should be standardized, while making necessary adjustments based on characteristics of the particular situation. The first part should be comprised of presenting the situation overview, which details all relevant quantitative and qualitative information known at that time regarding what is occurring in cyberspace and in physical space, and its implications in terms of the organization. In order to streamline the discussion, the situation overview should be coordinated with the various parties prior to finalizing it, and it should include two levels:

a. Technological situation overview: the attack objectives and dates, the attackers, insofar as they are known, cyber assets that have been hit (particularly vital cyber assets), effects on core processes and services, the status of contending with the attack and communications with professional outside sources.

b. Situation overview of overarching aspects: including ramifications on the functional and business continuity, economic-business repercussions, media and spokesmanship aspects, legal aspects and more.

Diagram 11:

Cyber Situation Overview (example)

As of:______________________

Discussion topic	Brief situation report	Actions taken/planned
Time of the attack		
Attacker(s)		
Type of attack		
Cyber assets affected		
Attackers' objectives and demands		
Leaked information and data		
Affected services/processes		
Announcements and publicity		
Interfaces with outside sources		
Overarching aspects		

During the second part of the discussion, the implications and alternatives presented in the situation overview will be analyzed and decisions and recommendations for action will be made. Subsequently, a summary of the decisions reached should be written and disseminated to the relevant stakeholders, particularly with regard to tasks that must be performed.

Diagram 12:

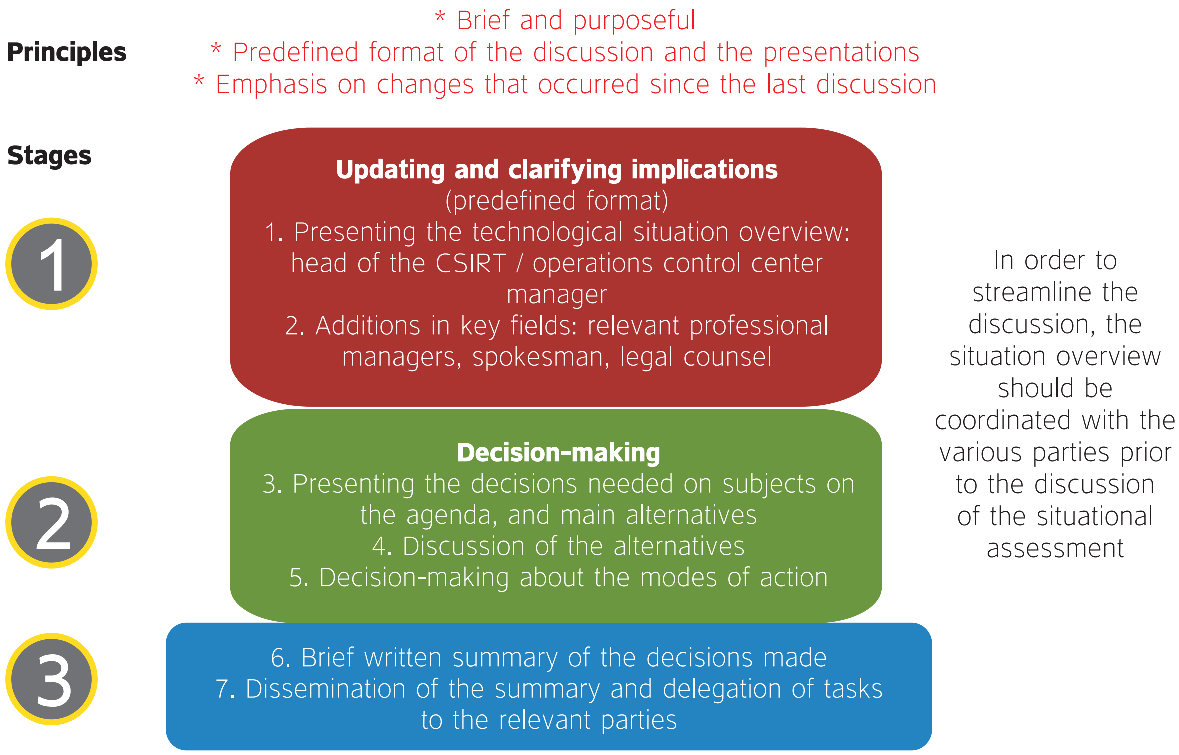
Issues for discussion during a situational assessment (example)

Capabilities in contending with the incident	Professional assistance needed (suppliers/ consultants/experts)	Necessary actions opposite outside sources, particularly the regulatory authority/ guidance unit	Necessary actions opposite customers
Priorities for reinforcing core processes and services	Decisions about operations in computerized systems (particularly vital cyber assets)	Decisions about actions relating to physical security	Implications in the context of manpower aspects
Updating the employees	Outside communications and Spokesman activities	Guidance with regard to information security aspects	Legal aspects
Actions to be taken			

In summary:

Diagram 13:

Situational Assessment Discussion



Principles

* Brief and purposeful
* Predefined format of the discussion and the presentations
* Emphasis on changes that occurred since the last discussion

Stages

1

Updating and clarifying implications
(predefined format)
1. Presenting the technological situation overview: head of the CSIRT / operations control center manager
2. Additions in key fields: relevant professional managers, spokesman, legal counsel

2

Decision-making
3. Presenting the decisions needed on subjects on the agenda, and main alternatives
4. Discussion of the alternatives
5. Decision-making about the modes of action

3

6. Brief written summary of the decisions made
7. Dissemination of the summary and delegation of tasks to the relevant parties

In order to streamline the discussion, the situation overview should be coordinated with the various parties prior to the discussion of the situational assessment

Appendix C: Questionnaire on the extent of the prepardeness for cyber crises (Top 10)

The questionnaire below is based on the concept presented in this document, and constitutes a tool for an organization's management to ascertain the degree of organizational prepardeness for cyber crises. The results of the questionnaire enable the management to rank the organization's prepardenessand to ascertain what actions must be taken to improve its preparedness.

The questionnaire may be used as is, or adjusted by each organization, and it is recommended that it should be carried out by those personnel in the organization who are responsible for functional continuity and cyber security, for risk management and emergency preparedness. Another possibility is receiving assistance from an objective, outside professional who will perform the assessment. Depending upon the nature of the organization, it is recommended to define a timeframe for completing the assessment (on average, annually), to be followed by drafting an improvement plan.

The questionnaire is based on a list of key topics, including segmentation into subtopics. In order to make it easy to fill in the answers and enable convenient display of the answers received (including graphic presentation), the questionnaire may be built in Excel or other application. An explanation about the grade calculation method is given at the end of the questionnaire.

List of topics in the questionnaire:

Organization responsibility [10% of the overall grade]

The questions below address the organizational responsibility for cyber crisis.

1. Has your organization defined functionaries and spheres of responsibility for preparedness for a **cyber crisis during routine times**?

a. Yes, at professional echelons and management echelons [3.34%]

b. Yes, at the professional echelon only [1.66%]

c. Yes, at the management echelon only [1.66%]

d. Not defined [0%]

2. Has your organization defined functionaries and spheres of responsibility **during a cyber crisis** (possible damage to a cyber asset deriving from deliberate activities)?

a. Yes, at professional echelons and management echelons [3.34%]

b. Yes, at the professional echelon only [1.66%]

c. Yes, at the management echelon only [1.66%]

d. Not defined [0%]

3. Has your organization defined "**core processes**" (processes that the organization conducts in order to achieve its key objectives and/or objectives defined for it by the regulatory authority)?

a. Yes, core processes have been fully defined [3.34%]

b. Yes, core processes have been defined partially/in specific instances [1.66%]

c. No, core processes have not been defined at all [0%]

Vital cyber assets [10%]

The questions below address the cyber assets that are vital to your organization. A vital cyber asset is an teleprocessing system (both hardware and software), which is being used, inter alia, to store, manage, process and transfer information, and/or to operate command and control, whose proper functioning is needed in order to maintain the continuity of a core process.

4. Have **vital cyber assets** been defined for your organization (by the organization or by the regulatory authorities)?

a. Yes, vital cyber assets have been fully defined [5%]

b. Yes, vital cyber assets have been defined partially/in specific instances [2.5%]

c. No, vital cyber assets have not been defined at all [0%]

5. Does your organization conduct tests in cooperation with **suppliers and service-providers** for the purpose of identifying threats and risks to vital cyber assets through the suppliers' systems/services?

a. Yes, fully conducted, including validation from time to time [5%]

b. Yes, carried out partially/in specific instances (only when beginning to work with a new supplier, or only for some suppliers) [2.5%]

c. No, not being conducted at all [0%]

Risk management [10% + 5% bonus]

The questions below address the cyber risk-management processes being performed in your organization (identifying cyber risks and assessing their severity and the repercussions deriving from these risks materializing).

6. At what frequency does your organization conduct a cyber risk-management process?

a. At least annually [5%]

b. Once every 2-3 years [3.3%]

c. Less than once every 3 years [1.6%]

d. Never [0%]

7. Bonus question: if cyber risk-management processes are being performed (clauses a-c under question 6), to what extent are the recommendations for risk-management processes being implemented?

a. Significantly implemented [5%]

b. Largely implemented [3.75%]

c. Moderately implemented [2.5%]

d. Marginally implemented [1.25%]

e. Not implemented at all [0%]

8. To what extent is your organization prepared, according to reference scenarios, for hostile cyber-attacks (playbooks for attacks against the organization and modes of implementation)?

a. Significantly [5%]

b. Largely [3.75%]

c. Moderately [2.5%]

d. Marginally [1.25%]

e. Not at all [0%]

Cyber states of alert [10% + 5% bonus]

The questions below address cyber states of alert in your organization. Cyber states of alert are "stages" reflecting the degree of vigilance and requisite preparedness. For example: "cyber routine" = no damage to cyber assets; cyber alert level A = substantive threat of damage to a vital cyber asset; cyber alert level B = damage to vital cyber asset(s), and so forth.

9. Has your organization defined cyber states of alert?

a. Fully defined [10%]

b. Partially defined/in specific instances [5%]

c. Not defined at all [0%]

10. Bonus question: if cyber states of alert are defined (clauses a-b under question 9), have the managerial authorities been defined for declaring and/or updating the states of alert?

a. Fully defined [2.5%]

b. Partially defined/in specific instances [1.25%]

c. Not defined at all [0%]

11. Bonus question: if cyber states of alert have been defined (clauses a-b under question 9), have the required actions been defined for each state of alert?

a. Fully defined [2.5%]

b. Partially defined/in specific instances [1.25%]

c. Not defined at all [0%]

Professional know-how [10%]

12. Is your organization using the "National Cyber Concept for Crisis Preparedness and Management" (this document)?

a. Yes [3.33%]

b. No [0%]

13. Is your organization using a cyber defense methodology (such as the CDMO which was disseminated by the INCD or other designated methodology)?

a. Yes [3.33%]

b. No [0%]

14. To what extent is your organization using recommended standards and work methods ("Best Practices") of an official organization, such as ISO standards, GDPR, NIST, privacy protection regulations?

a. To a very great extent [3.33%]

b. To a great extent [2.5%]

c. Moderately [1.66%]

d. Marginally [0.83%]

e. Not at all [0%]

Manpower [10%]

The questions below address manpower tasked with handling a cyber crisis, at the management echelon and at the professional echelon.

15. If your organization is defined as a "critical enterprise" have critical employees for ensuring the organization's functional continuity been designated for "round-the-clock on-duty" status?

a. Yes, Fully [3.33%]

b. Yes, partially /in specific instances [1.66%]

c. Not at all [0%]

d. Irrelevant (the organization is not defined as a "critical enterprise") [delete question and consider ranking the question based solely on questions 16-17]

16. Has your organization defined a **designated team** at the management echelon for the purpose of cyber crisis prepardeness and management?

a. Yes [3.33%] [If your organization is not defined as a "critical enterprise", write 5% instead of 3.33%]

b. No [0%]

17. Has your organization defined a professional-technological incident response team to provide a response in the event of a cyber crisis (can be an in-house response team or outsourced)?

a. Yes [3.33%] [If your organization is not defined as a "crititcal enterprise", write 5% instead of 3.33%]

b. No [0%]

Technologies and means [10%]

The questions below address technologies and means assimilated in your organization to enhance the level of cyber defense and to provide a response to attacks.

18. At what frequency are data backups being performed?

a. Constantly or daily [2.5%]

b. Weekly [1.66%]

c. Monthly and more [0.825%]

d. No backups are performed at all [0%]

19. Does your organization have technologies for monitoring and documenting operations in your computerized systems?

a. Yes [2.5%]

b. No [0%]

20. Does your organization have a separate DR site (Disaster Recovery) that is physically remote from the main site (for systems backups, information and business continuity)?

a. Yes [2.5%]

b. No [0%]

21. To what extent is your organization prepared at the logistics level to support the manpower needed to handle a cyber crisis (such as remote work, food, supplies, transportation, etc.)?

a. To a very great extent [2.5%]

b. To a great extent [1.875%]

c. Moderately [1.25%]

d. Marginally [0.625%]

e. Not at all [0%]

Receipt of assistance from outside sources [10%]

The questions below address the reliance on outside sources for the purpose of preparedness and handling of a cyber crisis.

Does your organization avail itself of tools and professional know-how of the INCD, the regulatory authorities, or of services of private companies for the purpose of:

22. Providing a response to cyber incidents?
Yes [2.5%] / No [0%]

23. Manpower training and instruction?
Yes [2.5%] / No [0%]

24. Training personnel in the organization?
Yes [2.5%] / No [0%]

25. The performance of audits?
Yes [2.5%] / No [0%]

Training and exercises [10% + 6% bonus]

26.Is cyber training and instruction being provided to functionaries (employees and management) in your organization (such as: to increase awareness and create an organizational culture revolving around cyber threats)?

a. Yes, frequently (including refresher courses) [3.33%]

b. Yes, occasionally/only in specific instances (such as only when hiring new employees) [1.66%]

c. No [0%]

27.At what frequency does your organization conduct cyber exercises?

a. At least annually [3.33%]

b. Once every 2-3 years [2.22%]

c. Less than once every 3 years [1.11%]

d. Never [0%]

28. Bonus question: If cyber exercises are being performed (clauses a-c under question 27), does the management echelon participate in these exercises? Yes [2%] / No [0%]

29. Bonus question: If cyber exercises are being performed (clauses a-c under question 27), do the professional-technological echelon(s) participate in these exercises? Yes [2%] / No [0%]

30. Bonus question: If cyber exercises are being performed (clauses a-c under question 27), do outside sources (suppliers) participate in these exercises? Yes [2%] / No [0%]

31.At what frequency does your organization conduct cyber audits (internal or independent)?

a. At least annually [3.33%]

b. Once every 2-3 years [2.22%]

c. Less than once every 3 years [1.11%]

d. Never [0%]

Cyber crisis management [10%]

32.Does your organization have a written plan (procedure) for cyber crisis management?

a. Yes [3.33%]

b. No [0%]

33.Has your organization defined contact people for reporting in the event that a cyber crisis emerges (who are the people you contact inside and outside your organization - regulatory authority, partners, customers, and how is contact made)?

a. Yes [3.33%]

b. No [0%]

34.Has your organization defined actions for returning to cyber routine and drawing conclusions while recovering from a cyber crisis (mode of formulating and assimilating the lessons learned)?

a. Yes [3.33%]

b. No [0%]

How to calculate the grade

The maximum grade in the questionnaire is 100% + 16% bonus.

Calculate each section by adding up the number of points (each question indicates the % being awarded).

Note: in the section "Manpower," there is a question relating to a "critical enterprise" (question 15) with a possible answer of "irrelevant." If your organization is not defined as a "critical enterprise" add up the points in the two remaining questions (16 + 17 only), and the maximum points for each of them is 5%. If your organization is defined as a "critical enterprise" add up the points for all three questions (15-17), and each question receives maximum points of 3.33%.

To obtain the overall grade for the questionnaire, sum up all percentages for all questions.

Example: sample calculation for the section cyber states of alert (questions 9-11) in the questionnaire

The section "cyber states of alert" awards a maximum of [10% + 5% bonus]. Therefore, for the answers described below (marked in yellow) the section will award 7.5% of the overall calculation (5% + 1.25% + 1.25%).

9. Has your organization defined cyber states of alert?

a. Fully defined [10%]

b. Partially defined/in specific instances [5%]

c. Not defined at all [0%]

10. Bonus question: if cyber states of alert are defined (clauses a-b under question 9), have the managerial authorities been defined for declaring and/or updating the states of alert?

a. Fully defined [2.5%]

b. Partially defined/in specific instances [1.25%]

c. Not defined at all [0%]

11. Bonus question: if cyber states of alert are defined (clauses a-b under question 9), have the required actions been defined for each state of alert?

a. Fully defined [2.5%]

b. Partially defined/in specific instances [1.25%]

c. Not defined at all [0%]

Cyber Israel

Prime Minister's Office
National Cyber Directorate

*9344
preparedness@cyber.gov.il
www.cyber.gov.il