ETSI TR 103 303 V1.1.1 (2016-04)

CYBER;
Protection measures for ICT
in the context of Critical Infrastructure

Reference
DTR/CYBER-0001

Keywords
Critical Infrastructure, Cyber Security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document reviews the roles and subsequent measures for the protection of any infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population, where such infrastructure is hereinafter referred to as Critical Infrastructure (CI). The resulting measures and processes for Critical Infrastructure Protection (CIP) where the CI in whole or in part is composed of ICT technologies using Cyber-Security mechanisms are defined and relevant mechanisms to be implemented are identified.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[i.2] Commission of the European Communities; COM(2006) 786 final; communication from the Commission on a European Programme for Critical Infrastructure Protection (Brussels, 12.12.2006).

[i.3] European Commission; SWD(2013) 318 final; Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure; Brussels, 28.8.2013.

[i.4] Public Safety Canada: "National Strategy for Critical Infrastructure".

NOTE: Available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

[i.5] Australian Government: "Critical Infrastructure Resilience Strategy", 2010.

NOTE: Available at http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlanAccessible.pdf.

[i.6] Japan Information Security Policy Council (ISPC): "Action Plan on Information Security Measures for Critical Infrastructure", 2005.

[i.7] ISO 27000 series: "Information technology -- Security techniques -- Information security management systems".

NOTE: ISO 27000 is a multipart standard. The reference is to the body of work prepared by ISO/IEC JTC1 SC27 in the domain of Information security management systems.

[i.8] ISO 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.9] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.10] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.11] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Infrastructure (CI): infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population

NOTE: Annex A of the present document presents a summary of existing definitions of CI that have informed the definition given above.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Access Control
CC	Common Criteria
CI	Critical Infrastructure
CIA	Confidentiality Integrity Availability
CIP	Critical Infrastructure Protection
CS	Critical Service
EAL	Evaluation Assurance Level
EU	European Union
ICT	Information Communications Technology
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
RBAC	Role Based Access Control

4 Identification and notification of Critical Infrastructure

4.1 Definition of CI

In order to identify CI it is essential to have a clear definition of what constitutes a critical service. This should be based upon the impact of a deliberate or accidental disruption to the service over a realistic timeframe. Critical services should then be further classified according to defined scales of impact should disruption occur. Subsequently, the infrastructure, whether physical or logical, essential to the operation of the service should be identified and similarly classified by impact to form CI.

NOTE: Whilst it is possible for a critical service to have no critical infrastructure (e.g. in the case of highly distributed systems where any critical impact on the service would require systemic failure across several resources) such systems and services are not addressed in the present document.

The process of CI classification enables the prioritization of protection efforts and investment decisions across CI. In working towards a classification it may be helpful to group critical services into sectors and sub-sectors to manage engagement efforts with relevant operators.

EXAMPLE: In the energy sector, a critical sub-sector is electricity, with the transmission or distribution of electricity to the nation representing a critical service. ICT which underpin this service, such as Industrial Control Systems, can then be identified and classified according to the impact of an attack on the availability or integrity of the system.

4.2 Identification of CI

Once definitions and criteria have been established it is crucial to design and implement a process to create and maintain an up-to-date record of CI. Stakeholders should be identified and provided with adequate mandates and resources to carry out this function. CI should not be considered in isolation but as part of the wider critical service that it supports.

At a minimum, the information captured should include the possible impact of an attack on CI, the owner of the CI, the location (where relevant) and a record of any dependencies or interdependencies required for continued operation.

The key questions to ask when identifying CI are:

- Are the impacts of a successful attack on the CI understood (including those resulting from interdependencies)?
- Have those impacts been used to properly categorize the CI?
- Have any dependencies (including technical, procedural and commercial) relating to the CI been captured and analysed?
- Have any interdependencies relating to the CI been captured and subjected to further analysis?
- Can the owner of the CI and its location be quickly ascertained?
- How frequently will the categorization of this CI need to be reviewed?

EXAMPLE: The generation of electricity is often dependent upon water supplies to provide adequate cooling of equipment in power plants. Conversely, the supply of water is dependent on electricity. Failure to identify this interdependence may result in the misclassification of CI and the implementation of inadequate security.

The process of identifying and categorizing CI should be iterative. Following the identification of CI dependencies it might become clear that there is a risk of common mode or cascading failure. The process should also be subject to audit on a regular basis to ensure it remains effective.

4.3 Notification of CI

Organizations should be familiar with the definition(s) of CI in their sector(s) and the government body acting as a point of contact in this area. Any organization believing that they either meet the relevant definition of CI or will do so in the near future should notify the relevant government body.

NOTE: Given the national significance of CI it is presumed that a government appointed body has responsibility for CI.

The key questions to consider when notifying CI are:

- At what stage should an organization notify the relevant body?
- Are organizations aware of the criticality thresholds and notification requirements for CI?
- How will organizations be persuaded to notify the relevant body when they meet the threshold for CI?

5 Security domains for CI protection

5.1 Review of CIA paradigm and its applicability in CI Protection

5.1.1 Overview

The conventional paradigm for provision of security features is CIA – Confidentiality, Integrity, Availability. This paradigm is conventionally applied in well defined domains and is often combined with known triples of {*domain, attack, countermeasure*}, such that in the confidentiality branch the triple {*confidentiality, interception, encryption*} will often appear. The characteristics of the common description of attacks in the CIA paradigm are typically centred on single attack vectors with Alice and Bob representing the end points of the to-be-secured transaction, and Eve representing the adversary. The application of CIA to CI is not in question as an attack that causes an outage of some part of the infrastructure could be as simple as a masquerade attack giving privilege escalation sufficient to override normal run-time security. Thus CIA should be considered as an essential building block in protection of CI.

The succeeding clauses summarize the aims of each of the CIA elements and their role in CI protection.

5.1.2 Confidentiality

The role of confidentiality protection is to ensure that information shared by Alice and Bob is intelligible only to Alice and Bob, and Eve, even if she can access that information, should be unable to understand the information in like manner to Alice and Bob. In Critical Infrastructure Protection (CIP) there are many parts of the management of the infrastructure that will be required to remain confidential and this may include configuration information of assets and their interactions.

Confidentiality also has a close relationship to privacy (shared meaning in US-English) and to core concepts such as unobservability, anonymity, pseudonymity and unlinkability. For a generic system the more of the system that is exposed then the greater risk there is that an attacker can identify an attack path. However, making the entire system "secret" does not make it more secure as it may lead the operators of the system to a false sense of security, this model of "security by obscurity" has been discredited over a number of years and whilst making everything public is not to be recommended it is reasonable to assume that those intending to attack a system, even if external to the system, have knowledge of the operations and architecture of a system.

The method of providing confidentiality of data either in storage or in transit for ICT in CI assumes that access control capabilities have been implemented in the first instance. As in all cryptographically protected schemes the method of protection will depend on overall trust and the cardinality of the relationships being protected.

EXAMPLE: The cardinality of the secured relationship in symmetric encryption is 1:1 (e.g. GSM), whilst for asymmetric encryption the cardinality is 1:m or m:1 (e.g. e-commerce). Where m:n relationships need to be secured they often first need to be normalized to sets of 1:m/m:1 relationships.

5.1.3 Integrity

5.1.3.1 Overview of the role of integrity

The role of integrity protection is that if Eve modifies data that that modification is detectable by Alice (and Bob if the data is exchanged with Bob).

NOTE: Bob can, as an actor, be Alice in the future. In other words, Alice stores data for future retrieval, in such a case future-Alice (Bob) should be able to detect if the stored data has been modified in the period between storage and retrieval.

5.1.3.2 Supply chain integrity

Supply chain integrity is a special case of integrity and addresses the entire chain to the end user. In this instance the term integrity is closer to the meaning of the term used in written English and refers to the overall trustworthiness of the supply chain and not to the stability of the supply chain. In cases such as Just in Time manufacturing attacks on the supply chain may be seen in a number of ways, for example an attack on the logistics tracking and planning may result in delays in delivery of components. Whilst such attacks are not necessarily likely to change a "normal" attack to one where the impact is sufficient to escalate the attack to one impacting critical infrastructure it is reasonable to consider attacks against supply chain integrity as likely to impact economic activity and in some cases (e.g. supply of medical relief) to impact the health of a population.

In many cases the supply chain has roots in natural phenomena - distribution of clean drinking water requires rainfall to be captured in lakes, rivers and reservoirs. A localized drought may impact the ability of CI to work but it is difficult to force nature to re-supply, however if periodic drought is possible the CI should take that into consideration in ensuring that sources of supply to meet demand can be integrated to the architecture, in other words if part of the supply chain is damaged that the overall CS can be maintained by appropriate design of the supporting CI.

5.1.4 Availability

The Availability element of the CIA paradigm covers a wide range of aspects including access control, identification, authentication, reliability, resilience and monitoring (for the purpose of assuring availability).

Any system that is classified as CI, and the services it supports, will almost inevitably become subject to a higher degree of accountability to 3rd parties than non-CI systems. As CI exploits have significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population, it is highly likely (certain) that government and their agencies will be concerned stakeholders. In consideration of the role of government to protect the economic activity of the nation or state, the safety, security and health of the population certain core requirements may have to be met for the provider of the CI. This may require that the provider/operator of the CI proves that the CI is adequately protected from unauthorized access.

Provisions for adequate CI protection may require to be independently verified. However, many of the existing schemes for such assurance are not scalable to very large and mutable systems. Of the existing standards based schemes in place the following may apply:

- ISO 27000 series [i.7]
  - The ISO 27000 series covers a wide range of security management, technical protection and controls capabilities. The set of controls identified in ISO 27001 for example cover a range of technology and organizational functions including access control, human resources, asset control, and incident management. These controls are mimicked in many national security assurance and evaluation programmes.
- ISO 15408-1 [i.8]
  - Commonly referred to as the Common Criteria (CC) in recognition of the willingness of signatories to recognize an evaluation made by one agency as valid for all signatories. The CC has been traditionally based on 2 types of evaluation product - a Protection Profile, and a Security Target with evaluation against a set of criteria and the depth of evaluation identified by discrete levels (e.g. Evaluation Assurance Level 5 (EAL5)). The evolution of CC towards a model of Community Protection Profiles (cPPs) is underway that drives CC towards a more standards like model. The bulk of existing CC evaluations are against components rather than systems.

- ETSI Design for Assurance [i.9]
  - The Design for Assurance programme is an informal set of ETSI guidance and standards documents based on the Common Criteria with a focus on development of technical standards that may be used in support of a CC evaluation.
- ETSI Secure by Default [i.10], [i.11]
  - The ETSI Security by Default programme extends the models of CC, of the ISO 27000 series [i.7], and the design for assurance programme, to a philosophy in which real business problems are identified and security solutions to the problems are solved at root cause, rather than by applying patches or "stop-gap" measures to address particular issues. The emphasis is therefore on security mechanisms embedded in core device functions; supplied literally "by default" in products instead of being added afterwards via updates or complex configuration. The secure by default programme is designed for consideration in large systems.

5.2 Resilience

In like manner to CI integrity the problem of CI resilience is that the system is inherently mutable and in normal operations will be subject to stress that it will be expected to recover from.

6 Measures for CIP

6.1 Protection lifecycle

For any system that is at risk of attack a very simplified model of protection is that based on the sequence of events:

- Plan
- Detect
- React
- Recover

Each of these events is explored in more detail below. The key assertion is that any reaction without a plan, reaction without knowledge of what is being reacted to, and reaction without a means to recover, is an ineffective reaction.

6.2 Planning measures

6.2.1 Overview of planning

Planning ensures that protection measures are considered and implemented prior to any attack. In addition, it provides confidence that should a successful attack occur, it can be detected and managed in a reasonable timescale.

6.2.2 Business Objectives

The desired security outcomes or goals for the organization should be defined and agreed at board level (or equivalent) before investing in protective measures. These objectives are likely to be shaped by commercial opportunities as well as legal, regulatory and contractual (such as those stemming from a third party) obligations. In particular, organizations should be familiar with the applicable definition(s) of CI and any associated security requirements in the environment where they operate.

6.2.3 Asset Management

Assets, whether physical or logical, that support services meeting the relevant definition of CI should be captured along with relevant metadata. In particular, any dependencies or interdependencies should be analysed and fed into risk assessment activities. This will enable sensible risk management decisions, better incident response in the event of an attack as well as driving pragmatic investment decisions.

6.2.4 Threat Assessment

Information concerning threats to CI should be obtained from relevant sources and analysed to inform risk assessment and management activities. This information should be augmented with data gleaned from vulnerability assessments, penetration tests and situational awareness gleaned from local monitoring activities.

6.2.5 Risk Management

Risks which if realized, could impact the CI, should be continually identified, assessed and managed as part of normal business operations. This should encompass direct attacks and those resulting from disruption to any dependencies. Residual risks deemed acceptable should be used to inform incident response exercises.

Risk management activities should be clearly linked to relevant business objectives.

6.2.6 Incident response

The organization should have a regularly tested incident response plan in place, with assigned roles and responsibilities, to execute in the event of a successful attack. Some remedial actions, such as isolating systems which are under attack, may inhibit business functionality. These trade-offs should have been assessed and agreed, along with the criteria for when such a remedial action would be necessary.

The plan should establish which stakeholders would need to be informed in the event of an attack, the mechanisms to be used, the detail required and expected timescales. This should be regularly rehearsed with relevant parties.

6.3 Detection measures

It is essential in any system to recognize when it deviates from its normal state of operation and to determine if the deviation is the result of fault, error, or attack and to maintain a plan of intervention in each case.

Detection of a CI incident should be close to real time.

6.4 CIA based reaction measures

6.4.1 Integrity measures

6.4.1.1 Identification of stable state - integrity base point

It can be reasonably asserted that any large system is mutable by definition as devices are replaced, reconfigured, or quite simply fail, over the life of the system. In addition, in large organizations there will be changes of staff through normal turnover, illness, reorganization, working patterns (i.e. it is not possible for a single person to work 24 hours a day every day over the life a system therefore a role may be shared by many individuals) and such. The demands of economic growth further suggest that an organization or business sector cannot be static in order to remain competitive and reactive in a changing market. The recognition of this inherent mutability makes many means to determine change either irrelevant or impractical particularly those based on any conventional document based cryptographic tools. However, it can be suggested that in spite of mutability there is a broad concept of normal operation and thus it should be reasonable to expect to be able to identify deviation from this state, where this state is termed the integrity base point.

For any system classifiable as CI, as identified in the planning phase, the identification of the stable state is a prerequisite to determining it is under attack (see detection measures above). Given that immutability is not an achievable or particularly desirable state and that a mathematical statement of the stable or normal state is unlikely to be achievable or accurate the following guidelines should be addressed by the responsible parties of the system:

- Identification of normal usage patterns
- Fore-planning of exceptional usage patterns

NOTE: In transport systems passenger load is unevenly spread with peaks at fairly easy to predict times, however major events (e.g. sports events, cultural events) place stresses on the system that contradict the normal pattern. Without reasonable planning such events may be misinterpreted as an attack.

EXAMPLE 1: During the early days of telephone voting for TV broadcasts the load on the network was sufficient to be viewed by the system as an attack and the resultant system defence mechanisms to limit access nearly led to catastrophic collapse of the national telecommunications network (a domino like effect of one subnetwork closure passing load that led to each subsequent subnetwork being closed).

EXAMPLE 2: A transport network may exhibit severe delays, potentially gridlock, if diversions either planned or made randomly by drivers, or by algorithms in satellite navigation software, as a result of road closure or accident (including by hostile acts) are not considered as normal behaviour even if their impact is damaging to one of the principles of CI.

- Identification of normal hysteresis level in the system
  - This requires knowledge of how long the system requires to become stable (i.e. to resort to a normal state) after an impulse like stimulus (e.g. a step change in network traffic loads either predicted or exceptional).
- Identification of standard deviation from normal behaviour in the system
  - Normal behaviour, as suggested above, is rarely constant or static but operates within certain bounds. Knowledge of these bounds to determine normal versus exceptional behaviour is essential to determine if the behavioural changes in the network lead to CI risk.
- Identification of long term trends in the system (including seasonal trends)
  - As above but noting that there may be seasonal changes in the expectation of normal.

In taking account of the above factors it is essential that the responsible parties address these questions across their entire supply chain and their target deployment environment.

Any system that is classified as CI may be dependent on a number of external stakeholders, that are not classified as CI, for which disruption may act as a side-channel attack on the primary CI system. Whilst overall system resilience can be addressed by using multiple sources of supply in the supply chain and alternative routing of products and services (as part of the onward supply chain) not all of the partners in the supply chain may be considered as CI.

EXAMPLE 3: The financial trading system of London is dependent on the availability of the financial trading systems of Frankfurt, New York and Tokyo (amongst others). An attack on one of these partner systems where they are not ranked as CI in the UK may lead to a breach of CI in the UK as a result of how they are interconnected. It is noted for this example that international financial security is directly impacted by the financial security of any one nation to a greater or lesser degree based on the level of trade.

6.4.1.2 Identification of manipulation of system - loss of system integrity

In a document structured world where for an arbitrary length input to a hashing function a fixed length output (the hash) is created such that any change in the input will result in a change of the output (the hash) with the condition that it is infeasible from examination of the change in the hash to falsely represent the change in the input. Quite simply there is no reasonable way to mathematically identify a hash of the system that can be used to determine if a change has occurred if the system is mutable. Thus a document structured world cannot be assumed for CI.

6.4.1.3 Recovery of compromised system - reinstatement of base point

As noted in clause 6.5 regarding recovery the recovered system should exhibit the same overall behaviour but may achieve that in a different way from before the CI attack. In such an event the same steps as determining the initial stable state have to be taken.

6.4.2 Availability measures

6.4.2.1 Access control measures

The base security model for any "at risk" system is to give access to system components and operations on a "need to know" basis. Given the mutability of CI systems in terms of staffing and capability the selection of an access control model is complex. Whilst some systems may require physical isolation and demand only physical access with detailed multi-factor authentication schemes in place, the reality of large scale integration of ICT capabilities suggests that the norm will become that all systems will have some form of remote control or remote monitoring in addition to direct onsite control and monitoring. Where systems tend towards wholly virtualized with autonomic management of instantiation of components (e.g. for load balancing) it may be difficult to identify the physical location of all critical system components at any point in time.

Actions which impact the system should be accounted for. This may be achieved by simple logging but as the risk from exploit increases the evidential nature of accounting records in identifying fault or attack also increases which may require that accounting records become both tamper resistant and able to retain evidence of tampering attempts.

EXAMPLE: If accounting records can be tampered to mask activity the ability to identify attacks (see Detection Measures above) may be invalidated and the exposure to critical risk magnified.

Role Based Access Control (RBAC) measures may be considered as the baseline. However, the assignment of critical control roles cannot be overly broad - i.e. not all users can have administrator rights. A prerequisite of any AC system (e.g. RBAC) is that users are identified and authenticated in order to prevent masquerade (Alice claiming to be Bob) and privilege escalation (Alice claiming the higher access rights assigned to Bob). Wherever possible authentication should be based on "strong" methods, i.e. cryptographic measures, as opposed to username-password combinations. However, where passwords are adopted measures should be taken to minimize the likelihood of weak passwords being used to access the system.

6.4.2.2 Critical instance override of access control

Access control systems should not inhibit access where an override may be necessary to allow for instances such as providing critical care or to prevent escalation of an incident.

EXAMPLE: It may be necessary for an actor not known to the system to access a patient record in a CI-labelled health system in order to give appropriate medical intervention (failure to do so may result in one or more fatalities).

If AC is overridden there should be records maintained (as far as is possible) of the extent of the override and the circumstances examined once the system has recovered to inform revised access control rules for similar circumstances in the future.

6.5 Resilience and recovery measures

When a system has been compromised it is reasonable to assume that when it is recovered it will perform the same set of functions but the means to perform those functions will be different from those used prior to the compromise.

EXAMPLE 1: A system that has been compromised by exploitation of a particular weakness (e.g. the Heartbleed attack on the openSSL library) may be recovered to a system updated to be immune to the exploited weakness with no change in overall "normal" functionality.

EXAMPLE 2: A system may be compromised by exploit of the trust in the root key of a PKI system and will be recovered to a new root key and re-signed certificate chain with no change in overall "normal" functionality.

EXAMPLE 3: A system with a centralized datacentre structure exploited by breaking links to the central point may be recovered to a distributed datacentre and multi-access virtualized resource pool with no change to overall "normal" functionality.

The key points for successful resilience and recovery are:

- Has the underlying attack been defeated?
- Has the weakness or set of weaknesses in the system that allowed the attack to be launched been isolated?

- Has the weakness or set of weaknesses that allowed the attack been removed?

NOTE 1: It may in some cases be impossible to remove exploitable weaknesses in a system without invalidating the system, or the redesign of the system may not economically viable to remove the exploitable weakness.

EXAMPLE 4: Cars crash into one another in part as a result of their complexity, in part because the primary controller is a fallible human, and in part because they share roads with cars driving in the opposite direction with only a line of paint to separate them. Reducing complexity, removing driver infallibility, and removing shared road space are either infeasible or economically inviable.

- Have relevant stakeholders and partners been informed?

- Have the systems of relevant stakeholders and partners been immunized in like manner?

NOTE 2: If an attacker has exploited systems using "strategy A" which have been successfully immunized against, it is essential that all connected and stakeholder systems that are vulnerable to the same "strategy A" have to be similarly immunized in order to defend against future attacks where "strategy A" is used as a side-channel attack at a related stakeholder.

Annex A:
Review of existing CI definitions

Whilst a simple definition of critical infrastructure is ideal it is clear that there is no commonly agreed one although many concepts are shared. Table A.1 takes some of the common definitions and whilst it is clear that there is a geographic dimension in each (i.e. the definition addresses a particular nation state or federation/union of nation states) removal of these aspects allows a common definition that may be applicable to all nation states.

Table A.1: Comparison of definitions

Definition	Source	Keywords and concepts
An asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.	[i.1], [i.2]	Loss of infrastructure leads to significant negative impact.
Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	[i.3]	As above but with some restriction to nationally owned or managed assets and appears to exclude assets under private or corporate ownership and management.
Processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life and adverse economic effects.	[i.4]	As above with concentration on national security (Canada).
Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.	[i.5]	As above with concentration on national security (Australia).
Infrastructure which offers the highly irreplaceable service in a commercial way is necessary for people's normal lives and economic activities, and if the service is discontinued or the supply is deficient or not available, it will seriously influence people's lives and economic activities.	[i.6]	As above but adding the non-governmental sector.

Common themes across all of the definitions collated in table A.1 suggest that a unified definition, without geographical specialization (i.e. not explicitly mentioning Australia or Canada or the United States or the EU), can be proposed.

The guiding principles to derive a common definition include the elements listed below:

- Loss or damage to the infrastructure element will lead to (significant) negative impact on one or more of the following:
  - Economic activity of direct and indirect stakeholders

NOTE 1: The stakeholders may be direct (e.g. owner/operators, customers) or indirect (e.g. citizens impacted by economic downturn which they did not contribute to) and may be a country/nation-state/region or a business sector but the definition of who is a stakeholder is not restricted.

  - The safety of the population
  - The security of the population
  - The health of the population

The infrastructure that may be considered as critical is not fixed. As technology and society changes the influence of technologies on the economy of a nation-state will change. It is reasonable to suppose that technologies in support of the distribution of clean water and adequate food supplies will always be considered as part of critical infrastructure thus transport and power, similarly the technologies to support health care of the populace will be considered as critical. More critically in some aspects the infrastructures required to maintain the safety and security of the populace need to be considered as critical. Evolving economic behaviour has moved to the Internet, in extension of the service market and of the distribution of goods (e.g. many entertainment media are delivered across the internet). Data centric services have also become a core of economic activity through initiatives such as openData thus that data infrastructure becomes critical to the maintenance of economic activity.

NOTE 2: The infrastructure is not limited to physical elements but may include virtual elements and the associative links between them.

CIs are generally considered to be large in extent supporting very large populations where the population may refer to number of people, transactions, devices, or in other words where the impact of loss or damage is significant.

Annex B: Bibliography

NIST: "Cyber-Physical Systems Homepage".

NOTE: Available at http://www.nist.gov/cps/.

NIST et al.: "Cyber-physical systems".

NOTE: Available at http://cyberphysicalsystems.org/.

NIST: "Foundations for Innovation in Cyber-Physical Systems Workshop", March 2012.

NOTE: Available at http://events.energetics.com/NIST-CPSWorkshop/index.html.

National Science Foundation: "Cyber-Physical Systems Virtual Organization".

NOTE: Available at http://cps-vo.org/.

Executive Order no. 13636: "Improving Critical Infrastructure Cybersecurity, DCPD-201300091", February 12, 2013.

NOTE: Available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Presidential Policy Directive 21 (PPD-21): "Critical Infrastructure Security and Resilience".

NOTE: Available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Public Safety Canada: "Action Plan for Critical Infrastructure (2014-2017)".

NOTE: Available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf.

History

Document history		
V1.1.1	April 2016	Publication