关键信息基础设施边界识别

研究报告（1.0版）

云南省互联网信息办公室

2019年6月

前　言

为有效落实关键信息基础设施（以下简称“CII”）保护措施，提高工作效率，CII运营者和保护部门应梳理出哪些网络设施、信息系统应被纳入CII保护范围。为了解决这个问题，网络安全领域广大从业人员从多方面进行了探索和研究。目前来看，从保障关键业务持续、稳定运行的角度出发，厘清CII与关键业务的支撑和依赖关系，或为识别CII边界提供具有启发性的方案。

2018年至今，在国家互联网信息办公室指导和支持下，云南省互联网信息办公室组织开展了“省域关键信息基础设施安全保障体系建设试点”工作。试点工作开展过程中，云南省互联网信息办公室联合深圳市腾讯计算机系统有限公司以及云南省内部分重点行业、企业对CII边界识别方案进行了探索与研究，实践与完善，形成了《关键信息基础设施边界识别研究报告（1.0版）》。该报告根据《中华人民共和国网络安全法》对CII的定义和保护CII的根本目的，结合国内外相关研究基础，从CII的形态与本质、CII受到攻击后的表现形式以及CII对关键核心业务的支撑模式等三个维度出发，阐释了基于信息/数据流的CII边界识别原理、识别流程和识别方法，并结合实践应用给出了CII边界识别具体案例。随着CII边界识别技术的不断完善和改进，被保护对象越来越得以明确，保护要求和保护技术措施切实得以落实，将进一步推进CII保护工作的发展。

版权声明

主要编写人员：秦小伟、胡容铨、冯燕春、胡红升、王东明、李璐瑶、姚相振、于盟、唐旺、李世淙、谭元翼、王二州、周晓龙、王彬筌、刘文胜、史波良、鲍文平

主要支撑单位：深圳市腾讯计算机系统有限公司、云南中烟玉溪卷烟厂、云南电网有限责任公司、富滇银行股份有限公司、中国移动通信集团云南有限公司、中国电信股份有限公司云南分公司、云南能投集团、云南日报报业集团、云南省电子政务网络管理中心、昆明地铁运营有限公司、昆明信息港传媒有限责任公司、玉溪市电子政务网络管理中心。

目 录

名词和缩略语

一、名词

1、关键信息基础设施

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的网络设施、信息系统。

2、关键信息基础设施元素

对构成关键信息基础设施的网络设施、信息系统的统称。其中，网络设施是指连接通信信息网络（互联网、物联网、工控网、专用网等）的基础性网络设施，以及在上述网络中对信息数据进行发送、传输、控制等操作的网络设备；信息系统是指由计算机软硬件、数据、规章制度等组成的按照一定规则运行的功能单元。

3、关键信息基础设施边界

识别关键信息基础设施元素的分界线，用于将关键信息基础设施元素同其它信息基础设施区分开来，以明确关键信息基础设施保护范围，确定被保护的关键信息基础设施保护对象。

4、业务信息

业务核心功能正常运行所必须的信息数据的统称。

5、业务信息流

业务信息从产生到终止，在整个生命周期内的流动轨迹。

二、缩略语

CII：关键信息基础设施（Critical Information Infrastructure）

BI：业务信息（Business Information）

BIF：业务信息流（Business Information Flow）

OMS：运行管理系统（Operation Management System）

一、关键信息基础设施及其边界识别

（一）什么是关键信息基础设施

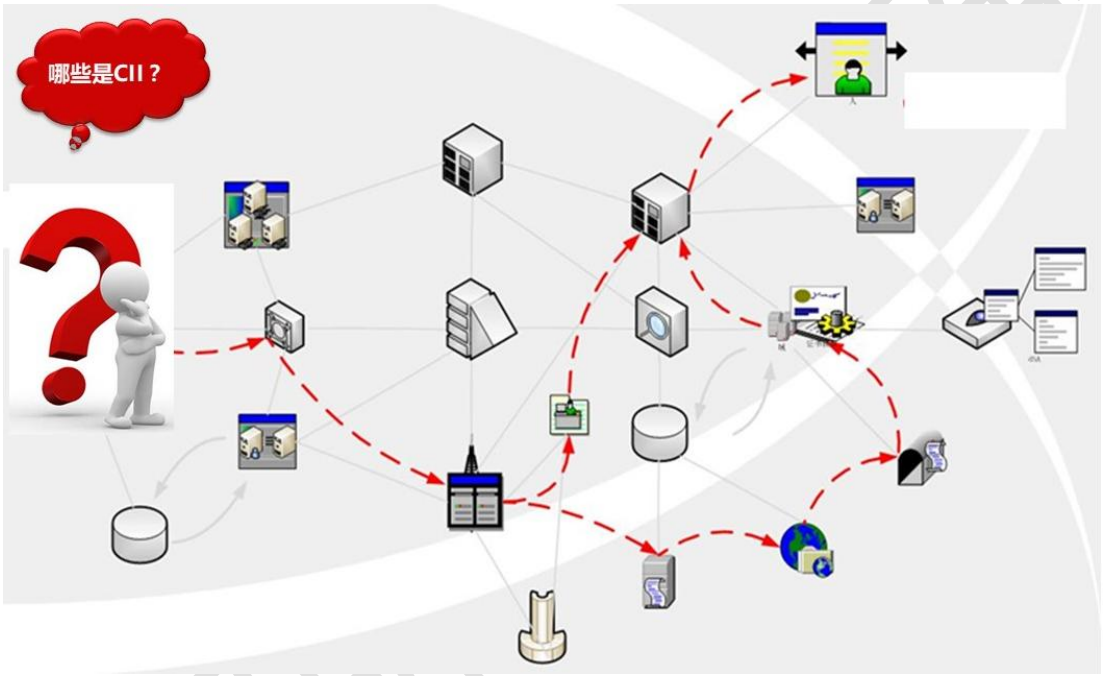
2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上发表重要讲话时指出，金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标，必须采取有效措施，切实做好国家关键信息基础设施安全防护。2017年6月1日正式施行的《中华人民共和国网络安全法》规定，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施实施重点保护。

2017年7月，国家互联网信息办公室向社会公开征求对《关键信息基础设施安全保护条例（征求意见稿）》的意见。《关键信息基础设施安全保护条例（征求意见稿）》对关键信息基础设施的定义做了阐述：关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能会严重危害国家安全、国计民生、公共利益的网络设施、信息系统等。

（二）什么是关键信息基础设施边界

在CII运营者的所有信息基础设施中，有一些网络设施、信息系统对保障关键业务持续、稳定运行是非常关键（Critical）的，有些仅仅是重

要（Important）的，还有一些是不重要（UN-important）的。开展CII边界识别就是将关键业务持续、稳定运行所必须的网络设施、信息系统同其它信息基础设施区分开来，明确保护对象，确定保护范围。边界内的网络设施、信息系统是构成CII的元素集合，是重点保护对象，如图一所示。因此，识别CII边界是开展CII保护工作的前提和基础，具有重要意义。



图一：CII边界示意图

（三）关键信息基础设施边界识别的意义

1、制定保护政策的依据

明确CII边界是制定CII保护政策、实施CII保护规划的前提，如果CII边界尚没有明确，开展CII保护工作将会缺乏针对性和科学性。比如，为CII采购产品和服务，可能影响国家安全的，应通过国家安全审查；CII

在境内运营中收集和产生的个人信息和重要数据，确需向境外提供的，应当进行安全评估等，都需要在确认了哪些网络设施和信息系统属于CII的前提下进行。

2、构建保障体系的前提

CII保护离不开监测预警、应急处置、检测评估等安全保障体系的建设。CII边界不明确将会给国家征集CII信息、构建国家关键信息基础设施安全保障体系带来一定困难。

3、落实保护措施的基础

开展CII保护的目的是为了保障关键业务稳定、持续运行，支撑关键业务的网络设施、信息系统一旦发生安全事件都可能对关键业务造成重大影响，这就让其它网络设施、信息系统上面的保护措施成为了“马奇诺防线”。因此，只有厘清关键业务与CII的支撑和依赖关系的前提下，明确CII的边界，制定保护措施，保障CII边界范围内的所有网络设施、信息系统安全运行才可以保障关键业务稳定、持续运行。此外，厘清关键业务与CII的支撑和依赖关系，也是确保CII现有安全体系和安全措施不遭到破坏的必要条件。否则，不仅起不到重点保护的作用，还可能会破坏已有的安全运行体系。

4、开展检测评估的需求

开展CII安全检查和检测的目的是为了有效落实保护方案，保障CII持续、稳定运行。因此，CII安全检查和检测需聚焦在关键业务安全运行至关重要的网络设施、信息系统之上。在不清楚哪些网络设施、信息系统

属于CII的情况下开展检查检测，扩大或者缩小检查范围，不但不能作为评估关键业务是否安全的有效依据，还可能威胁到关键业务本身安全运行，违背开展CII保护的初衷。

（四）关键信息基础设施边界识别面临的挑战

根据行业和领域的重要性确定CII运营者相对容易。例如，电网及大型发电厂、基础电信运营商、大型银行、航空枢纽、高速铁路、水利设施、云服务平台企业、大型能源矿产等，这些运营者所运营的关键信息基础设施一旦发生安全事件将可能严重危害国家安全、国计民生和公共利益。

然而，确定CII边界却是一个相对复杂的问题。首先，信息基础设施及其支撑的业务会变化，运营者也会更替，这将会改变关键业务与CII的支撑和依赖关系，进一步改变关键和非关键的元素，这就要求CII边界识别是一个动态、持续的工作。其次，要保障关键业务安全，就需要梳理出支撑该关键业务安全运行的所有网络设施和信息系统，因为任一网络设施、信息系统遭到攻击或者数据泄露都可能使其它设施的安全防御措施成为“马奇诺防线”。最后，信息与通信技术（Information and Communications Technology, ICT）和操作技术（Operation Technology, OT）具有的复杂性和不确定性以及二者在关键业务中的融合也会给CII边界识别带来困难。

1、需要保障业务安全

国家开展CII保护是为了保障那些可能涉及国家安全、国计民生、公共利益的关键业务安全正常运营，促进关键业务持续、稳定和健康发展。但是，网络设施、信息系统安全不等于关键业务安全。保障关键核心业务

安全的重点在于保护好那些遭到破坏后会对关键业务造成严重危害的网络设施、信息系统。因此，对信息基础设施各组成元素的关键性评估，需要完整认识关键业务的业务链。然而，在相关主体认知和有关利益冲突下，制定可行、高效的关键性评估标准是一个巨大挑战。可能会出现，其中一些主体认为“关键”的要素，另外一些相关主体却试图避免其被确认为“关键”的。所以，相关主体在梳理确定CII边界的时候，应从保障关键业务安全运行出发，建立动态协调和协同推进机制。

2、超出了关键基础设施的范围

在推行信息化的早期阶段，CII被认为是关键基础设施（Critical Infrastructure，CI）的一部分，保护范围比较明确。但是，随着信息化规模和水平的不断提高和数字经济不断发展，风险来源已远远超出CI范围，越来越多的风险来自于通信信息技术以及操作技术这种非传统安全领域的“虚拟实体”。例如，某些网络攻击和恶意软件会针对电力、燃气、水处理和化工厂的自动化控制系统进行信息窃取和数据篡改。所以，CII已经不仅是CI的一部分，其范围已超出了CI的边界范围。

3、信息不对称

CII边界识别工作必须具备一定业务专业知识，需要CII运营者在国家有关部门指导和监管下完成。重要行业和领域的主管部门可从宏观和整体角度对行业CII运营者重要性做出判断，但难以深入细致了解CII运营者业务运行的具体和实际情况，难以精准判定信息基础设施各组成元素的关键性，需要运营者的配合。然而，CII运营者往往缺少对国家网络安全整体

态势的有效认知，识别与被识别双方信息的不对称会造成CII识别结果和报备清单参差不齐、五花八门。所以，应建立以相关各方共同参与的识别机制，充分发挥运营者识别主体作用，科学、有效地识别CII边界。

4、需动态识别，持续迭代调整

目前来看，CII被攻击破坏、入侵、干扰的实际案例还不多，对于CII的识别，大多基于各相关方经过多轮研究和协商的最大共同认可来确定，其识别结果的客观性和有效性往往难以通过某单一验证机制进行确认。因此，CII边界识别往往需要在上一个识别结果基础上不断的迭代、更新和优化，根据信息基础设施各组成元素、网络安全动态风险及组织管理调整等因素，进行持续迭代更新调整。

（五）国内外研究现状

1、美国

1977年，美国总统关键基础设施保护委员会（President's Council on Critical Infrastructure Protection，PCCIP）指出，美国国家安全高度依赖信息和通信、银行和金融、能源、运输等关键基础设施，这些基础设施一旦遭到攻击会给整个国家带来严重后果，联邦政府需从“国家安全重点”的角度对其加以保护。据此，关键基础设施（Critical Infrastructure，CI）就被认为是那些一旦遭到破坏或摧毁，会对国家安全、经济发展或者公民健康造成严重影响的物质、设施、服务或者网络等，关键基础设施保护（Critical Infrastructure Protection，CIP）的概念被正式提出。

20世纪90年代中期，信息技术和互联网兴起，信息通信技术迅速渗透到社会各个方面，大幅度扩大了威胁的范围。人类拥有了通过虚拟的、非物理破坏的方式让关键基础设施停止运行的能力，因此，加强对关键基础设施的网络保护受到美国等发达国家的重视。1996年，时任美国总统克林顿发布第13010号行政令，指出关键基础设施要么建立在脆弱的系统上，要么受到系统监视和控制，极易遭受来自网络侧的虚拟攻击。从此，在网络侧加强对关键基础设施的保护成为CIP政策新焦点。

2001年美国“9·11事件”的发生，进一步提高了人们对关键基础设施脆弱性的认识。美国时任总统乔治·布什签署《爱国者法案》，将关键基础设施定义为“各种系统和资产的集合，包括虚拟和物质的。这些系统和资产对美国及其重要，其失效或者遭到破坏都会给国家安全、经济发展、公共安全造成负面影响”。此后，美国CIP政策虽多次调整，但都沿用了《爱国者法案》中对关键基础设施的定义。

现行的美国CI所包含的领域是2013年奥巴马政府颁布的第21号总统令确定的，该将化工、商业设施、通信、关键制造、大坝等16个行业纳入关键基础设施重点保护行业，如图二所示。

在识别上述领域和行业内的关键基础设施方面，美国政策可以概括为四个阶段，如图三所示。

第一阶段，2003年美国直接以“如果一个系统或资产遭到攻击，会对生命和财产带来灾难性的损失”设为判断标准。显然这个判断方法过于模糊，地方和行业难以准确理解，在随即开展的国家关键基础设施信息征集

的时候，各地上报的数据良莠不齐。这种方法可以概括为定义法，即直接简单的以关键基础设施的定义作为识别准则。

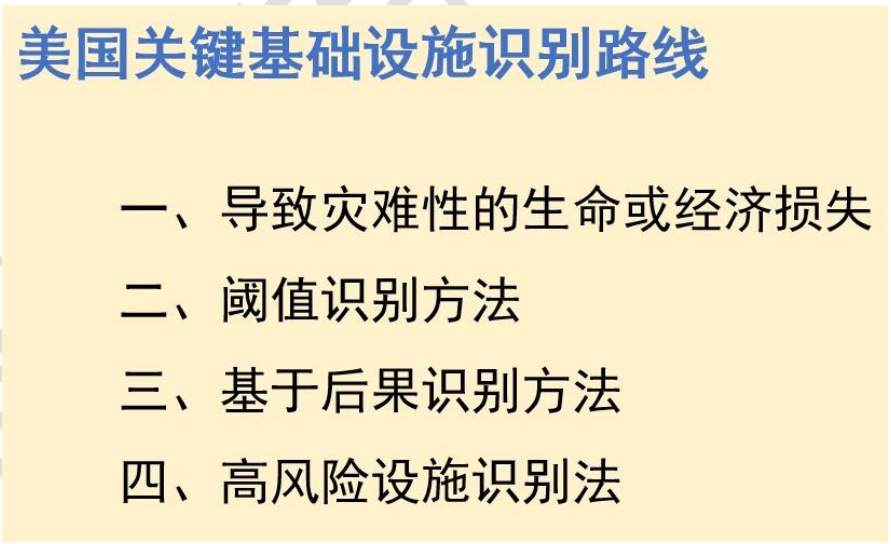
第二阶段，2004年美国发布了《识别国家级别的关键基础设施和关键资源指南》，首次提出了基于阈值的识别方法。基于阈值的识别方法明确给出了可量化的判断标准用于指导各州征集国家关键基础设施信息。比如，每年转账超过500亿美的证券服务商即可判定为国家关键基础设施，向超过4个州提供运输服务的公司即可判定为国家关键基础设施等等。该识别方法易于实施、简单明了，但缺点也非常突出。这种“一刀切”式的识别方法容易造成国家关键基础设施的遗漏，而且随着时间的推移阈值变化会非常大。

第三阶段，2009年美国提出了完全基于后果的识别方法，并建立了基于后果的认定准则：一是死亡情况，是指一旦某个系统或资产遭到攻击，会造成的死亡人数；二是经济损失，包括应急处置、系统恢复以及导致的上下游成本等；三是大规模撤离，是指事件发生以后造成周边居民大规模撤离；四是国家安全，是指造成国家安全能力的降低。

第四阶段，2010年美国对基于后果的关键基础设施识别方法又进一步改进和补充，提出了高风险设施识别方法。一些高风险的基础设施不一定同时满足基于后果的评估准则，但会对某个方面造成严重影响。例如食品安全不一定会造成多严重的经济损失，但是会造成大量人员伤亡；再比如金融系统遭到攻击不一定会造成人员伤亡和发生大规模撤离，但是会严重影响经济发展。

关键基础设施领域				主管部门
1996	2002	2003	2013	
	化工和危险材料	化工	化工	国土安全部
	商业设施	商业设施	商业设施	国土安全部
电信	信息和电信	电信	通信	国土安全部
		关键制造（2008）	关键制造	国土安全部
		大坝	大坝	国土安全部
	国防工业基础	国防工业基础	国防工业基础	国防部
应急服务	应急服务	应急服务	应急服务	国土安全部
石油天然气、电力	能源	能源	能源	能源部
银行和金融	银行和金融	银行和金融	金融服务	财政部
	农业和食品	农业和食品	食品和农业	农业与卫生服务部
政府	政府	政府设施	政府设施	国土安全部
	公共健康	公共健康与保健	保健与公共健康	卫生服务部
		信息技术	信息技术	国土安全部
		核反应堆、材料和废弃物	核反应堆、材料和废弃物	国土安全部
交通运输	运输	运输系统	运输系统	国土安全部和交通部
	邮政和船运	邮政和船运		
供水系统	水	饮用水和水处理系	水及污水处理系统	环境保护局

图二：美国关键基础设施行业变迁图



图三：美国关键基础设施识别路线演进图

2、欧盟

欧洲共同体委员会2004年10月20日发布了《打击恐怖主义活动，加强关键基础设施保护》，将关键基础设施定义为：“关键基础设施是由如果被破坏或摧毁，会给公民的健康、安全、稳定或成员国政府有效运转造成严重影响的物理和虚拟的信息设施、网络、服务和资产。关键基础设施横跨经济的诸多部门和重要政府服务”。

2005年，欧盟委员会发布《欧洲关键基础设施保护计划》，确定了关键基础设施的范围和领域：

（1）能源，石油和天然气生产、提炼、处理和存储，包括运输管道、发电、输电等。

（2）信息和通信技术，包括信息系统和网络保护，设备自动化和控制系统，互联网，固定电信服务，移动电信服务等。

（3）水，包括饮用水供应，水质控制、水量控制等。

（4）食品，包括食品供应和食品安全保护。

（5）健康，包括医疗和医院护理，药品、血清、疫苗和药物等。

（6）金融系统，包括支付服务和体系，政府财政调配等。

（7）公共和法律秩序安全，包括维持公共和法律秩序的安全，司法和拘留管理等。

（8）民政管理，包括政府、应急服务，邮政和快递等。

（9）交通，包括公路交通，铁路交通，航空运输，内河航运，远洋和近海航运等。

（10）化学和核工业，包括化学以及核材料的生产、运输、存储、加工等，危险药品的运输管道等。

（11）太空和研究。

确定行业和领域后，在识别具体信息基础设施方面，欧盟早期提出了一种网络架构分析方法。根据通信网络中核心网络设施和附加组件所承载负载的大小，通过检查、分析，制定国家网络基础设施视图。这个方法的缺点是不依赖于关键业务,不涉及关键业务的分析,只关注网络基础设施，目前没有成员国使用这种方法

2014年12月，欧盟发布了《关键基础设施资产和服务识别方法》，用来指导各成员国识别关键的信息基础设施。方法建议分成两步，首先识别关键业务，然后基于业务识别哪些资产属于这些业务，进而可考虑为关键的资产和服务。同时，《关键基础设施资产和服务识别方法》也给出了是否为关键资产和服务的评价原则，一是参考消费者体验，二是故障是否导致服务中断。

2016年7月6日，欧盟通过首部网络安全法《网络与信息系统安全指令》，旨在加强基础服务运营者、部分数字服务提供者的网络与信息系统安全。其中基础服务包括：能源、交通、银行业、金融市场基础设施、健康产业、饮用水供给、数字基础设施。基础服务运营者认定标准有三个：一是所提供的服务对于重要的社会、经济活动是必须的；二是该服务的提供依赖于网络与信息系统；三是一旦发生网络安全事故，将对该服务的提供产生破坏性影响。

3、中国

虽然我国开展CII保护工作晚于欧美等发达国家和地区，但是近年来的工作进展较快。2016年4月，习近平总书记在“4·19”讲话中指出，金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标，必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。2016年11月7日，《中华人民共和国网络安全法》正式颁布，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施实施重点保护。2017年7月，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》，在《中华人民共和国网络安全法》的基础之上，对可能存在CII的行业和领域作了详细描述：

（一）公共通信和信息服务，包括电信、互联网、广播电视等。

（二）能源，包括电力、石油天然气、石化等。

（三）交通，包括铁路、公路、水运、民航、城市轨道交通等。

（四）水利。

（五）金融，包括银行、证券、保险等。

（六）公共服务，包括卫生、教育、社会保障、市政服务等。

（七）电子政务，包括海关、税务等。

（八）国防科技工业。

在CII识别认定的问题上,国家互联网信息办公室于2016年制定了《关键信息基础设施确定指南（试行）》和《国家网络安全检查操作指南》。《关键信息基础设施确定指南（试行）》中，将CII类型分为网站类、平台类和生产业务类等三大类,设置了可纳入国家关键信息基础设施得信息基础设施指标要求。例如：日均访问量超过100万次的网站，一旦发生网络安全事件会影响超过100万人正常工作和生活的信息平台，注册用户超过1000万或者日均交易额超过1000万元的电子商务平台等。《国家网络安全检查操作指南》对识别CII的流程作了进一步描述：第一步确定关键业务；第二步确定关键业务相关的信息系统或工业控制系统；第三步根据关键业务对信息系统或工业控制系统的依赖程度以及发生安全事件之后的损失和影响后果来判定是否属于关键基础设施。

2016年6月，中央网信办组建国家关键信息基础设施安全检查办公室（以下简称“检查办”），并组织开展了我国第一次全国范围内的CII摸底大检查工作。由于各地各行业各领域报送的CII信息参差不齐，与预设情况有一定差距，更加凸显了CII边界识别的重要性。如何有效识别认定CII边界迫在眉睫。为此，检查办专门设置“识别认定组”，开展关键信息基础设施边界识别认定研究工作。期间，检查办先后围绕CII保护基线和CII识别认定方法制定了有关文件，用于指导地方和行业开展工作。

（六）小结

综上，CII或CI保护的根本目标是保障涉及国家安全、国计民生、公共利益的关键业务正常运行。因此，从确保业务安全稳定的角度出发，梳

理CII与关键业务的支撑和依赖关系,或为识别CII边界提供富有启发性的解决方案。因此，CII边界识别可遵循下列步骤：

第一，确定重要行业和领域。《关键信息基础设施安全保护条例（征求意见稿）》对可能存在关键信息基础设施的行业和领域做了较为详细的描述：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等。

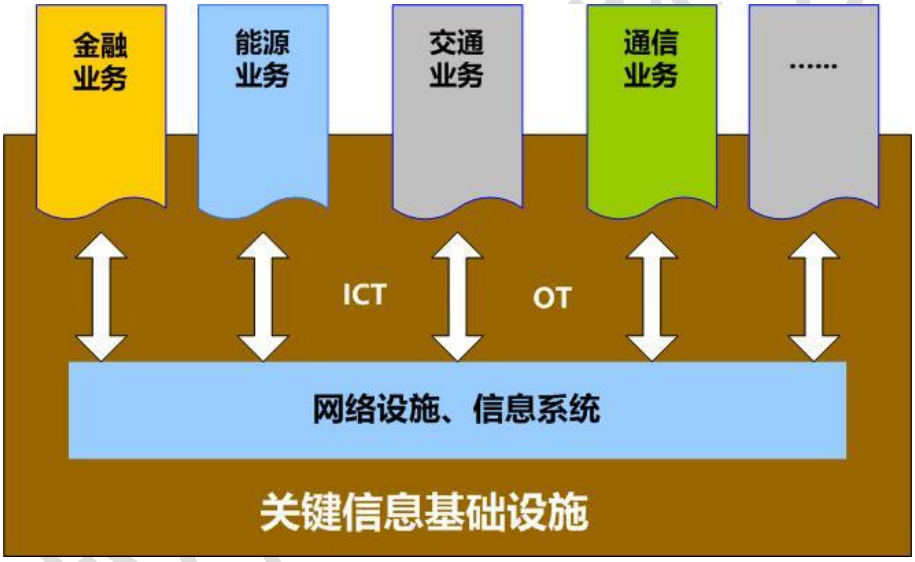
第二，确定关键业务及其运营者。重要行业和领域重要并不代表行业和领域内的所有业务都是关键的,识别关键业务及其运营者就是将上述行业和领域内的影响国家安全、国计民生、公共利益的关键核心业务识别出来并明确运营者。

第三，确定CII边界。根据业务特征和业务运行逻辑，将关键业务持续、稳定运行所必须的网络设施、信息系统从运营者的其它信息基础设施元素中识别出来，明确保护对象，确定保护范围。

二、关键信息基础设施边界识别原理

（一）CII 形态构成

CII在形态构成上是网络设施、信息系统或者由网络设施、信息系统组成的集合，是业务的信息化支撑部分。CII采用一定规模、有组织、有架构的信息网络体系，通过信息获取、信息传递、信息处理、信息再生、信息利用等手段，极大的提高业务各种行为效率，支撑业务自动化、智能化、快速高效运行，如图四所示。



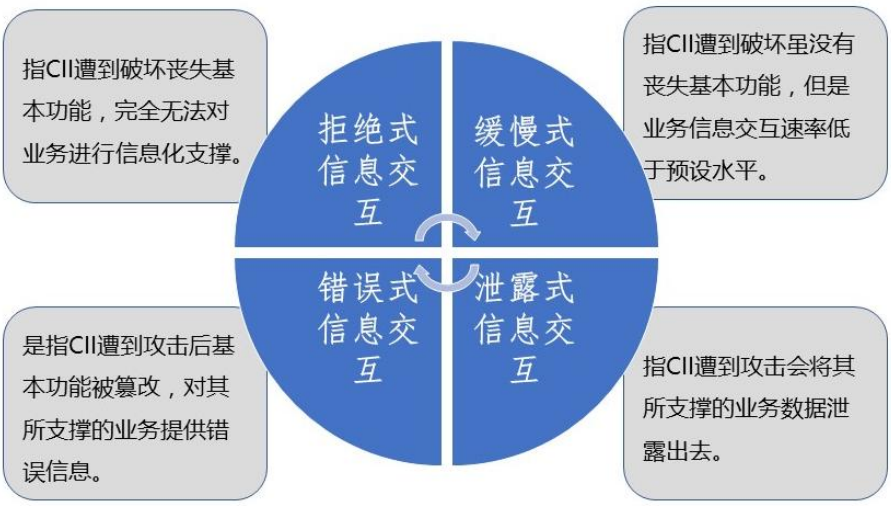
图四：CII形态和本质

CII与业务之间的关系就体现在这种信息化支撑上,保护CII的目的就是避免因发生网络事件导致信息获取、信息传递、信息处理、信息再生和信息利用等环节无法正常运行，进而对业务持续、稳定运行造成灾难性影响。

信息处理的不同环节与业务流程紧密相关，每个环节都有相应的网络设施和信息系统支撑来完成的。在关键核心业务的整个流程内，参与信息处理的网络设施、信息系统就是CII可能的最大边界范围。如果范围内的网络设施、信息系统对保障业务的正常运行至关重要，就应当被纳入关键信息基础设施的保护范围。

（二）CII 遭到攻击后的表现模式

保护CII的目标是避免关键业务的信息化部分遭受攻击、丧失功能或者数据泄露，保障业务信息化部分正常运行。CII一旦遭到攻击无法正常运行，信息获取、信息传递、信息处理、信息再生和信息利用等环节便受到影响，CII支撑业务的环境就会遭到破坏，最终表现形式是下列四种，如图五所示：



图五：CII遭到攻击后的表现模式

1、拒绝式信息交互

拒绝式信息交互是指CII遭到破坏后丧失基本功能，完全无法对业务进行信息化支撑。比如，铁路的信号控制系统遭到破坏以后，无法对列车发出预警或者停车信号；灾情预警系统遭到破坏后，无法提供险情预警数据，也无法发出控制指令；云服务出现故障，拒绝任何形式的访问请求等。

2、缓慢式信息交互

缓慢式信息交互是指CII遭到破坏虽然没有丧失基本功能，但是业务信息交互速率远低于预设水平。例如，运营商的数据管道业务是按照既定速率将业务交付的信息从发送端提供给接收端，当支撑上述业务的CII受到攻击以后，这种信息交互速率就会降低；网络购票业务需要在客户端和服务器之间传输信息，如果支撑上述功能的CII遭到攻击后，信息传输速率就会降低，表现为用户购票效率降低。

3、错误式信息交互

错误式信息交互是指CII遭到攻击后基本功能被篡改，对其所支撑的业务提供错误信息。比如，电力控制系统是保障电力调度安全，一旦遭到攻击后会对供电系统发出错误指令；导航系统为用户提供准确位置信息，受到攻击后会提供错误位置信息；网上支付业务是将资金划到用户指定的账户上，如果系统遭到攻击，可能会给业务提供错误信息，表现为将错误数量的资金转移到错误的账户上等。

4、泄露式信息交互

泄露式信息交互是指CII遭到攻击会将其所支撑的业务信息泄露出

去。例如，数据存储业务是云的一个重要功能，正常情况下只与授权用户之间进行信息交互，受到攻击后可能会被非法用户窃取信息，即发生数据泄露；电子医疗系统存有大量患者信息，如果遭到攻击，会发生个人隐私数据泄露；网上招生报名系统记录大量考生信息，如果系统遭到攻击，会发生考生信息泄露等。

（三）CII 支撑业务的形式

CII与业务之间的依赖关系就体现在信息化支撑上，具体表现为下列九种场景，或者是下列九种场景的任意组合，如图六所示。

信息产生：是指根据业务需求，按照预设信息模式产生信息数据，使之能够有效地存储、流转等，满足业务各个应用环节的需求,又称信息起源或者信息设计。

信息采集:是指根据业务需求,将设计好的信息数据收集起来的过程，又称信息获取。

信息处理：是指从大量的、可能是杂乱无章的、难以理解的信息数据中抽取并推导出某些特定的有价值、有意义的信息数据。在表现形式上可能是采集、存储、检索、加工和变换。

外部信息采集：是指根据业务自身的需求，收集除自身设计以外的信息数据。

信息整合：是指把在不同信源的信息数据收集、整理、清洗，转换后加载到一个新的信源，为信息处理提供统一视图。

信息呈现：是指按照业务预设功能，将信息起源阶段所要达到目标的

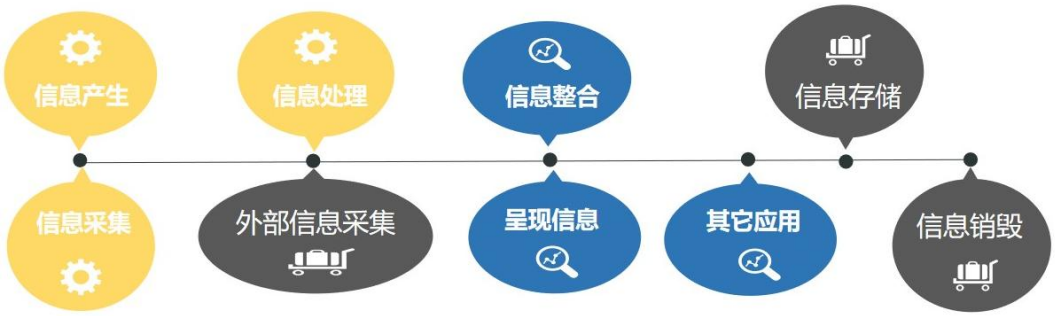
最终展示。

其它应用：是指将信息数据用于业务自身以外的其它用途。

信息存储：是指将信息数据以某种格式记录在介质上。

信息销毁：是指信息消亡的过程，分为两种，一种是可恢复删除，另外一种是不可恢复删除。

当CII受到攻击造成上述任一环节发生故障时，就会损害业务的持续、稳定运行。

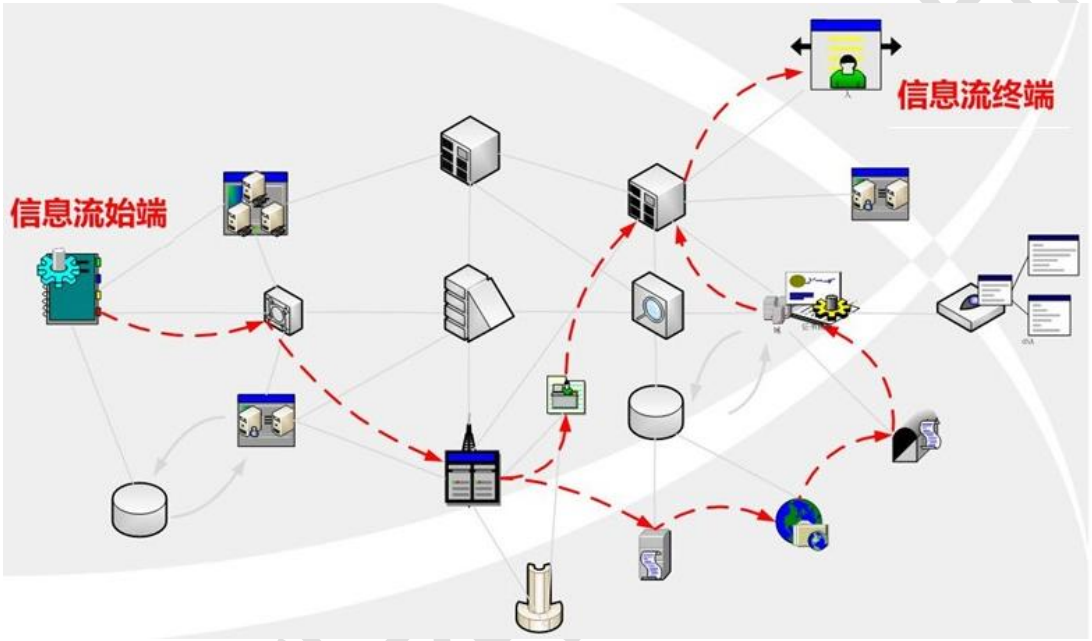


图六：CII对业务的支撑模式

（四）CII 边界识别方法

经过以上分析可以得出，CII在形态构成上是网络设施、信息系统或者由网络设施、信息系统组成的集合。CII在本质上属于业务的信息化部分，一旦遭到攻击、丧失功能或者数据泄露会严重影响业务的信息化部分正常运行，进而给业务造成严重影响。CII对业务的支撑模式以及CII遭到攻击后的表现形式，最终也都体现在对信息的处理上。

因此，关键业务正常运行所需的信息流，从初始到终止所流经的网络设施、信息系统便组成了CII最大可能边界，如果上述网络设施、信息系统对保障关键业务正常运行至关重要，就应当纳入CII保护范围，如图七所示。



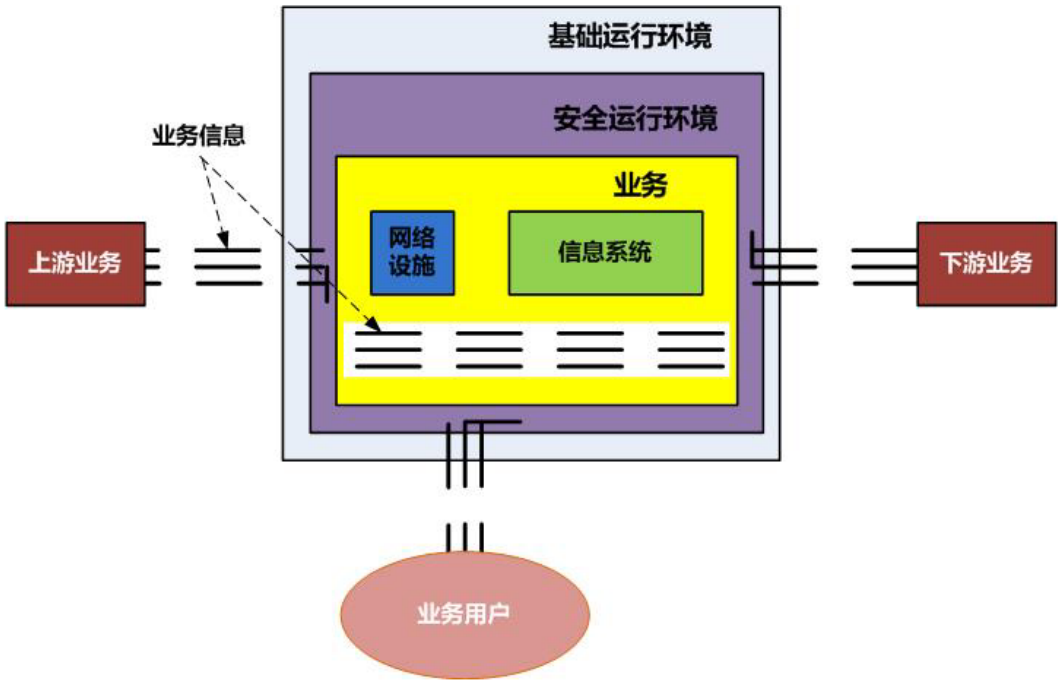
图七：CII边界确定示意图

（五）CII 边界识别模型

业务、网络设施、信息系统、业务信息、安全运行环境、基础运行环境，是识别CII边界需要考虑的六个方面，如图八所示。识别CII边界，首先要识别关键业务，关键业务是核心要素，其它要素都是围绕着关键业务产生的:即网络设施、信息系统是关键业务正常运行所必须的信息化部分，与业务是信息化支撑关系;业务信息是关键业务正常运行所必须的数据资

源，同时也是网络设施、信息系统实现对关键业务信息化支撑的纽带和桥梁，网络设施、信息系统按照业务运行逻辑和功能划分对业务信息进行处理，包括设计、存储、整合、删除等操作，实现了对关键业务核心功能的信息化支撑；安全运行环境主要包括安全设备、控制措施、安全策略、规章制度等，用于保障关键业务的信息安全；基础运行环境为关键业务正常运行提供电力、空调等基础条件。

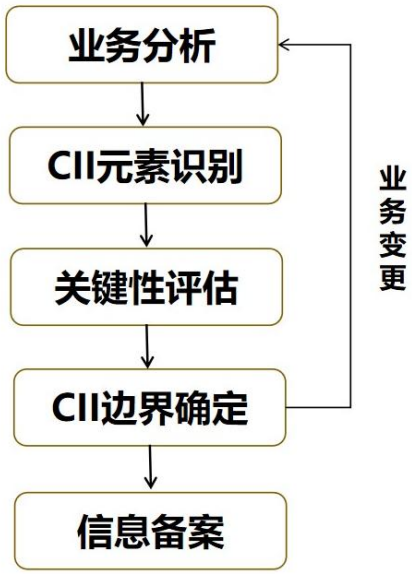
基于上述概念，网络设施、信息系统是CII元素的候选对象，其中一旦遭到攻击、丧失功能或者数据泄露会严重影响关键业务持续、稳定运行的网络设施、信息系统纳入CII保护范围。



图八：CII边界识别模型

三、关键信息基础设施边界识别流程

综合以上分析可以得出，可以按照图九所示流程梳理关键业务持续、稳定运行所必须的网络设施、信息系统。



图九：CII边界识别流程

（一）业务分析

业务分析的主要目的是调查了解关键业务运行架构、运行逻辑和开展范围，对业务核心功能和业务信息化运行情况进行梳理，是开展CII边界识别的基础工作，包括业务识别、业务梳理、业务特征识别和业务信息化描述四个部分。

1、业务识别

业务识别是指将CII运营者所运行的关键业务识别出来的活动。关键业务由行业主管部门结合CII运营者客观情况认定，组织开展CII边界识别

工作应以行业主管部门认定的关键业务为基准。

2、业务梳理

根据关键业务所在的行业领域特点，调查了解关键业务运行情况，包括业务开展范围，业务服务对象以及上下游业务运行情况。

3、业务特征识别

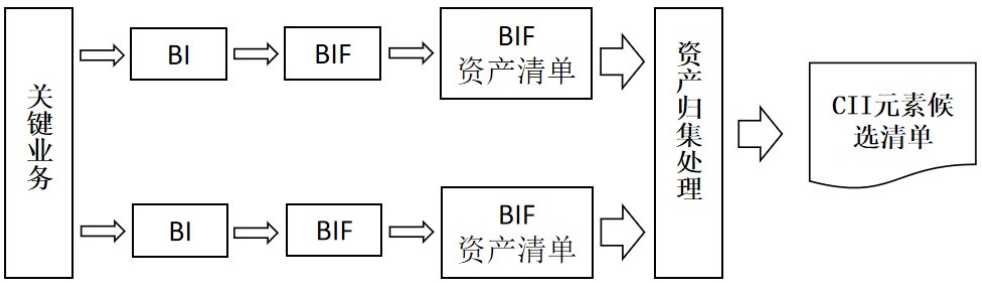
根据业务基本情况，调查了解业务运营的地理位置、岗位设置和岗位职责等方面信息，梳理业务运行逻辑，识别业务核心功能。

4、业务信息化描述

根据业务基本情况和业务特征，调查了解业务的信息化建设、信息化管理、信息化运维等方面信息，获得支撑业务运行的网络拓扑结构，网络设施、信息系统部署情况。

（二）CII 元素识别

CII元素识别的主要目的是梳理支撑关键业务持续、稳定运行的网络设施、信息系统，确定CII元素候选清单，是开展CII元素关键性评估的准备工作，包括BI识别、BIF识别和CII元素归集三个部分，如图十所示。



图十：CII元素识别流程

1、BI 识别

根据业务基本情况、业务特征和业务信息化运行情况，梳理关键业务持续、稳定运行必不可少的BI，获得BI种类和用途。

2、BIF 识别

梳理BI从产生到终止的全生命周期内的流动轨迹，即BIF。调查了解BIF上的网络设施、信息系统部署详情，获得相应的资产清单。

3、CII 元素归集

对所有BIF上的网络设施、信息系统进行归集处理，得到支撑该关键业务的网络设施、信息系统清单，即CII元素候选清单。

（三）关键性评估

关键性评估是指评估CII候选元素一旦遭到破坏、丧失功能或者数据泄露对关键业务持续、稳定运行所造成的影响。评估指标包括但不限于业务可用性、业务完整性和数据机密性，评估结果为关键的CII候选元素纳入CII保护范围。

1、评估指标

业务可用性:业务可用性遭到破坏是指CII遭到破坏后丧失基本功能，完全无法对业务进行信息化支撑。比如，铁路的信号控制系统遭到破坏以后，无法对列车发出预警或者停车信号；灾情预警系统遭到破坏后，无法提供险情预警数据，也无法发出控制指令；云服务出现故障，拒绝任何形式的访问请求等。

业务完整性：业务完整性遭到破坏是指CII遭到破坏虽然没有完全丧

失对业务的信息化支撑，但是业务功能受到影响，比如信息交互速率远低于预设水平、某子功能完全缺失等。例如，运营商的数据管道业务是按照既定速率将业务交付的信息从发送端提供给接收端，当支撑上述业务的CII受到攻击以后，这种信息交互速率就会降低；电视直播业务是将电视信号从服务端推送到客户端，如果支撑上述功能的CII遭到攻击后，信息传输速率就会降低，表现为用户接到的电视信号停顿；铁路购票系统具有现场购票、网络购票和电话购票三种功能，支撑网络购票的CII遭到攻击后，网上购票功能可能会完全丧失或者购票缓慢等。

数据机密性：数据机密性遭到破坏，是指CII遭到攻击后基本功能被篡改，对其所支撑的业务提供错误信息，或者将业务信息泄露出去。比如，电力控制系统是保障电力调度安全，一旦遭到攻击后会对供电系统发出错误控制指令；导航系统为用户提供准确位置信息，受到攻击后会提供错误位置信息；数据存储业务是云的重要功能，正常情况下只与授权用户之间进行信息交互，如果受到攻击可能会将信息提供给非法用户，即发生数据泄露。

2、评估方法

按照表一所示，针对每一个CII候选元素，分析其一旦遭到破坏、丧失功能或者数据泄露对业务可用性、业务完整性和数据机密性所造成的影响；对任一评价指标造成影响的CII候选元素其关键性评估结果应为关键；对所有评价指标都无影响的CII候选元素其关键性评估结果应为非关键。将评估结果为关键的CII候选元素纳入CII元素清单。

表一 CII元素关键性评估表

序号	评估对象	评估指标		
		业务可用性	业务完整性	数据机密性
1	网络设施	影响/否	影响/否	影响/否
2	信息系统	影响/否	影响/否	影响/否

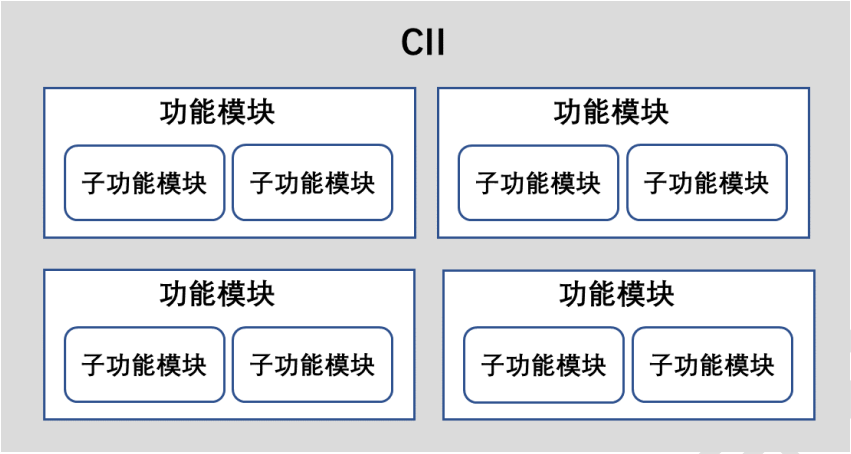
（四）CII 边界确定

CII不是简单的由一系列网络设施、信息系统组成的“杂乱无章”的设备清单。CII首先以“功能”为最小组成模块，小功能模块组成大功能模块，以此递归，最后组成一个支撑关键业务的完整CII。每一个功能模块的信息包括该功能模块的名称、所包含的子功能模块以及说明文档，最小的功能模块仅由名称和说明文档组成。功能模块的名字应是该功能模块主要功能的高度概括，比如边界路由表信息采集模块。每一个模块的说明文档应对该模块的主要功能进行介绍，如图十一所示。

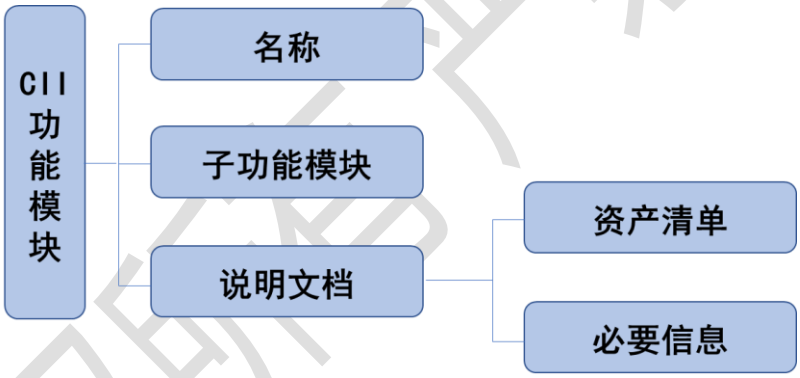
CII的名称应是其所支撑的关键业务的高度概括，比如电力调度指挥平台，高速铁路预警系统等。CII的说明文档除了涵盖功能模块说明文档所有信息以外，还应包括所支撑业务情况介绍等，如图十二所示。

（五）信息备案

根据CII元素，确定CII边界，并将CII边界文档化，形成一套指导开展CII保护的文件，备案信息应当包括：运营者信息、专门网络安全管理机构信息、所属行业信息情况说明、关键业务说明、CII所支撑、承载的业务情况介绍、CII清单和边界说明等。



图十一：CII边界呈现示意图



图十二：CII边界信息图

四、应用案例

现以电力行业为例，介绍“基于信息/数据流的关键信息基础设施边界识别方法”。

案例中所列出的数据已经过脱敏处理，不代表真实情况，主要用于解析本研究报告所提出的边界识别方法，但不影响案例的说明属性。

（一）业务分析

1、业务识别

电网运行稳态监视与控制是电网安全运行的重要保障，负责监测电力生产、电力传输、电力配送环节的运行态势，及时处理发现的安全隐患，一旦遭受网络攻击，会给整个电力系统的稳定运行造成严重影响。

2、业务梳理

电网运行稳态监视与控制业务分为省、市两级，分别由省级电力调控中心和市级电力调控中心负责运营，主管机构是省电力总公司。

省级电网运行稳态监视与控制业务主要负责管内220kV及以上电厂、变电站及部分110kV电厂、变电站稳态监测与控制，并将信息及时与管内各供电局共享；市级电网运行稳态监视与控制业务主要负责管内部分110kV电厂、变电站及35kV以上电厂、变电站稳态监测与控制，并将所管区域内的信息数据上送到省级电力调控中心，整个业务运行框架如图十三所示。

3、业务特征识别

电网运行稳态监视与控制业务主要负责调管范围内的电网运行态

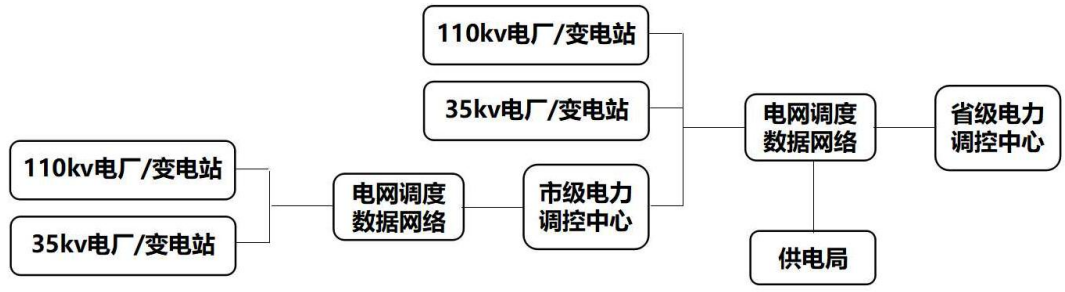
势监测和事故分析，控制开关刀闸、投切电容器、调节发电机组输出功率，确保机组总输出与用电总负荷实时平衡，保证电网电压质量合格，是整个电网安全运行的基础和核心保障。

4、业务信息化描述

部署在各电厂、变电站的监控系统和测控装置将各电厂、变电站运行态势信息通过电网调度数据网络自动上送给各级电力调控中心，最后数据归集到省级电力调控中心。

省级电力调控中心利用电网稳态监视与控制平台对收集到的电网运行态势数据实时智能化处理，实现对整个电网运行态势的感知。

电网稳态监视与控制平台在电网运行态势的基础之上，结合其他外部数据，比如风功率预测系统、OMS等上报的数据，做出精准判断，并通过调度主站系统、智能远动子站系统、厂房子站系统将调控、调度指令下发给部署在各发电厂、变电站的监控系统和测控装置。



图十三：电网运行稳态监视与控制业务运行架构

（二）CII 元素识别

1、BI 识别

（1）监测信息

电能量计量信息：电能量计量信息主要用于监测实时用电量，为电力调度提供依据。

继电保护信息：继电保护信息主要实现对供电安全装置的运行状态、动作行为进行监测，在电网故障时则进行快速的故障分析。

相量测量信息和行波测距信息：相量测量信息和行波测距信息主要用于对故障地点进行定位。

（2）控制信息

控制指令：控制指令，用于开合刀闸、投切电容器。

发电计划指令：发电计划指令，用于控制各发电机组的发电量。

（3）辅助信息

天气、水纹信息：用于辅助下发控制指令。

（4）共享信息

电网运行态势信息，用于各供电局实时掌握用电量，为制定行业发展规划提供依据。

2、BIF 识别

（1）电能量计量信息：电能量数据采集器、电能量数据处理系统、电能量纵向互联交换机、纵向加密装置、电力调度数据网、电网综合数据网、SAN交换机、数据中心、大屏显示与控制系统。

（2）继电保护信息：继电数据采集器、采集服务器、电力调度数据网、电网综合数据网、SAN交换机、数据中心、大屏显示与控制系统。

（3）相量测量信息：相量数据采集器、电力调度数据网、电网综合数据网、SAN交换机、数据中心、大屏显示与控制系统。

（4）行波测距信息：行波数据采集器、电力调度数据网、电网综合数据网、SAN交换机、数据中心、大屏显示与控制系统。

（5）天气、水纹信息：数据采集服务器、正反向隔离装置、电网综合数据网、大屏显示与控制系统。

（6）控制指令：电网运行控制系统、电力调度数据网、纵向互联交换机、发电厂/变电站端远动装置、发电厂计算机端监控系统、变电站测控装置。

（7）发电计划指令：电网运行控制系统、电力调度数据网、纵向互联交换机、发电厂/变电站端远动装置、发电厂计算机端监控系统、变电站测控装置。

（8）共享信息：数据中心、WEB系统、电网运行控制系统暂态监视与保信系统。

3、CII元素归集

对梳理出的资产去重、合并、归集得到支撑电网运行稳态监视与控制的CII元素候选清单如下：

数据采集服务器、行波数据采集器、继电数据采集器、采集服务器、电能量数据采集器、电能量数据处理系统、电网运行控制系统、电能量

纵向互联交换机、发电厂/变电站端远动装置、发电厂计算机端监控系统、变电站测控装置、纵向加密装置、正反向隔离装置、电力调度数据网、纵向互联交换机、电网综合数据网、SAN交换机、WEB系统、电网运行控制系统暂态监视与保信系统、数据中心、大屏显示与控制系统、电网运行控制系统。

（三）关键性评估

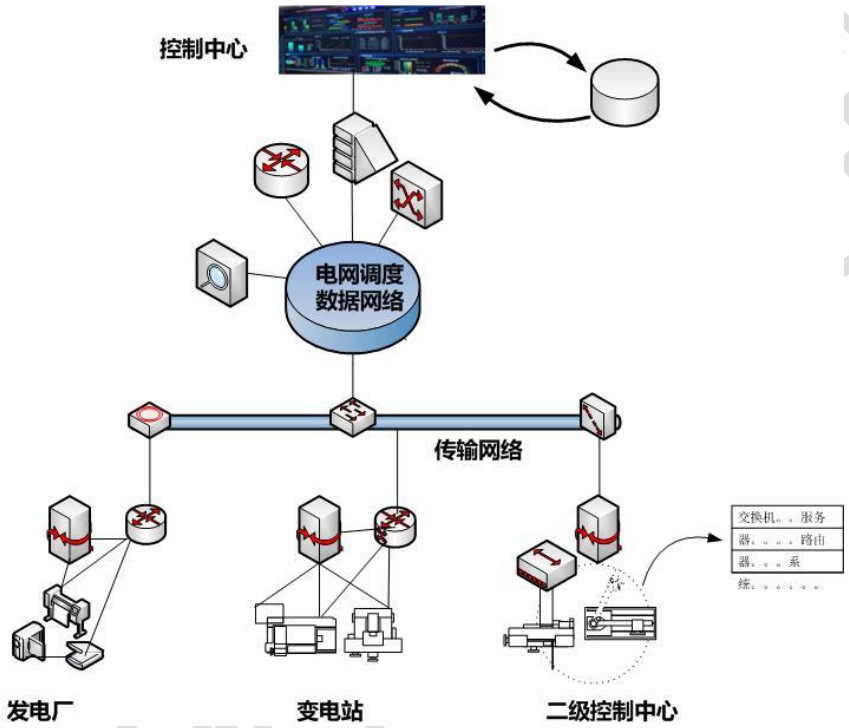
对梳理出的CII候选元素进行关键性评估，评估结果如表二所示。

表二 CII 元素关键性评估

类型	涉及信息系统和设备	评估结果（是/否关键）	边界范围（是/否）
终端设施	数据采集服务器	是	是
	行波数据采集器	否	否
	继电数据采集器	是	是
	电能量数据采集器	是	是
	电能量数据处理系统	是	是
	发电厂/变电站端远动装置	是	是
	发电厂计算机端监控系统	是	是
	正反向隔离装置	是	是
传输系统	电力调度数据网	是	是
	纵向互联交换机	是	是
	电网综合数据网	是	是
	SAN 交换机	是	是
后台系统访问端	电网运行控制系统	是	是
	电网运行控制系统暂态监视与保信系统	是	是
	数据中心	是	是
	大屏显示与控制系统	是	是
	WEB 系统	是	是

（四）CII 边界确定

支撑电网运行稳态监视与控制业务的CII元素（部分）网络拓扑结构如图十四所示。



图十四：CII（电网运行稳态监视与控制）元素网络拓扑结构

参考文献

1. International Standard Industrial Classification of All Economic Activities, ISIC Rev 4.0.

2. Efforts to Identify Critical Infrastructure Assets and Systems, 2009.

3. Security Guideline for Electricity: Identifying Critical Cyber Assets, 2007.

4. Critical Infrastructure: The National Assets Database, Office of Inspector General, 2007.

5. Developing the National Assets Database, 2006.

6. DHS List of Priority Assets Needs to Be Validated and Reported to Congress, 2013.

7. UK State Strategy for Critical Infrastructure, 2010.

8. Germany Critical Information Infrastructure Protection Plan, 2005.

9. The Russian Federation Information Security, 2000.

10. Operation Liberty Shield was a comprehensive national plan to protect the homeland during U.S. operations in Iraq.

11. Whitehouse Issues for Cybersecurity of Foreign Policy.

12. Lepinski, M. and S. Kent, “An Infrastructure to Support Secure Internet Routing”, RFC 6480, February 2012.

13. John, S., David, W., Randy, B. and Rob, A., “BGP Prefix Origin Validation”, RFC6811, October 2015.

14. Randy, B., “Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)”, RFC7115, March 2017.

15. Stephen, K. and Andrew, C., “Threat Model for BGP Path Security”, RFC7132, October 2015.

16. Steven, M., Randy, B. and David, W., “Security Requirements for BGP Path Validation”, RFC7353, October 2015.

17. Geoff, H. and George, M., “The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure”, RFC7935, September 2016.

18. Pradosh, M., Keyur, P., John, S., Dave, W. and Randy, B., “BGP Prefix Origin Validation State Extended Community”, RFC8709, March 2017.

19. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, May 2008.

20. Housley, R., “Cryptographic Message Syntax (CMS)”, STD 70, RFC 5652, September 2009.

21. Yan Pu, A. Nakao, “A deployable upload acceleration service for mobile devices,” Information Networking, IEEE International Conference on, pp. 350–353, Feb. 2012.

22. Y. Zhu, and A. Nakao, "Upload Cache in Edge Networks", Advanced Information Networking and Applications, IEEE International Conference on, Fukuoka, Japan, pp. 307-313, March 2012.

23. S. Raheel, R. Raad, C. Ritz, " Efficient utilization of peer's upload capacity in P2P

networks using SVC", Communications and Information Technologies, International Symposium on, Incheon, Korea, pp. 66-70, Sept. 2014.

24. P. Lettieri, and M. B. Srivastava, "Adaptive Frame Length Control for Improving Wireless Link Throughput, Range, and Energy Efficiency", INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 2, pp. 564-571, Apr 1998.

25. L. Peng and S. Li, "An Improved Algorithm of RTP Adaptive Transmission Control", International Conference on Genetic and Evolutionary Computing, Guilin, China, pp. 595-599, Oct. 2009.

26. J-Y park, J-S An, Y-N Han, S-J Lim et. al., "Throughput performance improvement of adaptive packet length allocation scheme in wireless data communication system," Proceedings of 1995 International Symposium on Communications. ISCOM'95, vol. 1, pp. 401-408, Dec. 27-29, 1995.

27. P. Lettieri, C. Fragouli, M. Srivastava, "Low Power Error Control for Wireless Links," In Proceedings of the Third ACM/IEEE International Conference on Mobile Computing and Networking 1997 (MobiCom'97), pp.139-150, Sep. 1997.

28. Ling-Jyh Chen, Tony Sun, and Sanadidi, M.Y., "Improving wireless link throughput via interleaved FEC", Computers and Communications, vol.1, pp. 539-544, Jul 2004.

29. 关键基础设施风险相互依赖性 : Risk and interdependencies in critical infrastructures 胡可斯塔德，于特内，瓦特恩崔亦谦 - 国防工业出版社

30. CIIP Guidelines Ver.3.0 ,The 9th ASEAN-Japan Information Security Policy Meeting October 20th, 2016

31. A Comprehensive Instrument for Identifying Critical Information Infrastructure Services, Luis Carlos Herrera Velasquez

32. Risks and Interdependencies in Critical Infrastructures- A Guideline for Analysis , Per Hokstad SINTEF Safety Research, Trondheim, Norway

33. Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1，National Institute of Standards and Technology，January 10, 2017

34. 国民经济行业分类（GB/4754-2011）。

致　谢

在本报告的研究、实践和制定过程中，得到了公共通信和信息服务、能源、交通、金融、电子政务等重要行业和领域的领导、专家、学者等的悉心指导与大力支持，编制组在此表示衷心感谢。

感谢云南中烟玉溪卷烟厂、云南电网有限责任公司、富滇银行股份有限公司、中国移动通信集团云南有限公司、中国电信股份有限公司云南分公司、云南能投集团、云南日报报业集团、云南省电子政务网络管理中心、昆明地铁运营有限公司、昆明信息港传媒有限责任公司、玉溪市电子政务网络管理中心等省域关键信息基础设施安全保护试点承担单位对边界识别方法进行的积极实践、应用验证，以及提出了建设性的意见和建议。

感谢国家计算机网络与信息安全管理中心云南分中心、云南省信息安全测评中心、上海交通大学云南（大理）研究院、深圳市易聆科信息技术有限公司和云南省互联网协会等科研机构和社会组织，为进一步改进和完善研究报告给予支持。