DOWNLOAD PDF CRITICAL INFORMATION INFRASTRUCTURES

Chapter 1 : What's critical about critical infrastructure?

Identification of Critical information infrastructure is the first step in the process to secure and protect the availability of critical assets. Several Member States have launched different initiatives regarding this topic while others are starting now to develop their own approaches. The.

CIP[edit] The U. CIP is a national program to ensure the security of vulnerable and interconnected infrastructures of the United States. Take, for example, a computer virus that disrupts the distribution of natural gas across a region. This could lead to a consequential reduction in electrical power generation , which in turn leads to the forced shutdown of computerized controls and communications. Road traffic, air traffic, and rail transportation might then become affected. Emergency services might also be hampered. An entire region can become debilitated because some critical elements in the infrastructure become disabled through natural disaster. The federal government has developed a standardized description of critical infrastructure, in order to facilitate monitoring and preparation for disabling events. The government requires private industry in each critical economic sector to: Assess its vulnerabilities to both physical or cyber attacks Plan to eliminate significant vulnerabilities Develop systems to identify and prevent attempted attacks Alert, contain and rebuff attacks and then, with the Federal Emergency Management Agency FEMA , to rebuild essential capabilities in the aftermath Infrastructure sectors[edit] CIP defines sectors and organizational responsibilities in a standard way: Note that CIP in this sector is different from energy security , which is the politics and economics of supply. Additionally, operating under the auspices of the Federal Energy Regulatory Commission is the North American Electric Reliability Corporation NERC , a non-profit organization that defines and enforces reliability standards for the bulk power system. Search and rescue teams formed from various emergency services coordinated by FEMA Federal and municipal services: They guarantee continuity of government at the federal, state, and local levels to meet for provision of essential services. This includes safe water systems and drainage. In the remit was expanded to include: Agriculture and food, with the Department of Agriculture overseeing the safe supply of meat, poultry, and egg products. National monuments and icons, under the Department of the Interior With much of the critical infrastructure privately owned, the Department of Defense DoD depends on commercial infrastructure to support its normal operations. The Department of State and the Central Intelligence Agency are also involved in intelligence analysis with friendly countries. It is going to be against commercial infrastructure". Later this fear was qualified by President Clinton after reports of actual cyber terrorist attacks in We lost our Pacific fleet at Pearl Harbor. In the past, the systems and networks of the infrastructure elements were physically and logically independent and separate. They had little interaction or connection with each other or other sectors of the infrastructure. With advances in technology, the systems within each sector became automated, and interlinked through computers and communications facilities. As a result, the flow of electricity, oil, gas, and telecommunications throughout the country are linkedâ€”albeit sometimes indirectlyâ€”but the resulting linkages blur traditional security borders. While this increased reliance on interlinked capabilities helps make the economy and nation more efficient and perhaps stronger, it also makes the country more vulnerable to disruption and attack. This interdependent and interrelated infrastructure is more vulnerable to physical and cyber disruptions because it has become a complex system with single points of failure. In the past an incident that would have been an isolated failure can now cause widespread disruption because of cascading effects. One catastrophic failure in this sector now has the potential to bring down multiple systems including air traffic control, emergency services, banking, trains, electrical power, and dam control. The elements of the infrastructure themselves are also considered possible targets of terrorism. Traditionally, critical infrastructure elements have been lucrative targets for anyone wanting to attack another country. Now, because the infrastructure has become a national lifeline, terrorists can achieve high economic and political value by attacking elements of it. Disrupting or even disabling the infrastructure may reduce the ability to defend the nation, erode public confidence in critical services, and reduce economic strength. Additionally, well chosen terrorist attacks can become easier and less costly than traditional warfare because of the interdependence of infrastructure elements. These infrastructure

elements can become easier targets where there is a low probability of detection. The elements of the infrastructure are also increasingly vulnerable to a dangerous mix of traditional and nontraditional types of threats. Traditional and non-traditional threats include equipment failures, human error, weather and natural causes, physical attacks, and cyber attacks. For each of these threats, the cascading effect caused by single points of failure has the potential to pose dire and far-reaching consequences. Challenges[edit] There are fears that the frequency and severity of critical infrastructure incidents will increase in the future. One reason for this is that a good understanding of the inter-relationships does not exist. There is also no consensus on how the elements of the infrastructure mesh together, or how each element functions and affects the others. Securing national infrastructure depends on understanding the relationships among its elements. Thus when one sector scheduled a three-week drill to mimic the effects of a pandemic flu , even though two-thirds of the participants claimed to have business continuity plans in place, barely half reported that their plan was moderately effective. CIP is important because it is the link between risk management and infrastructure assurance. It provides the capability needed to eliminate potential vulnerabilities in the critical infrastructure. CIP practitioners determine vulnerabilities and analyze alternatives in order to prepare for incidents. They focus on improving the capability to detect and warn of impending attacks on, and system failures within, the critical elements of the national infrastructure. Organization and structure[edit] PDD mandated the formation of a national structure for critical infrastructure protection. The different entities of the national CIP structure work together as a partnership between the government and the public sectors. In addition, there are grants made available through the Department of Homeland Security for municipal and private entities to use for CIP and security purposes. These include grants for emergency management, water security training, rail, transit and port security, metropolitan medical response, LEA terrorism prevention programs and the Urban Areas Security Initiative. These are national defense, foreign affairs, intelligence, and law enforcement. Each lead agency for these special functions appoints a senior official to serve as a functional coordinator for the federal government. A private sector counterpart, a Sector Coordinator, was also identified. Together, the two sector representatives, one federal government and one corporate, were responsible for developing a sector NIAP. Additionally the national structure must ensure there is a national CIP program. This program includes responsibilities such as education and awareness, threat assessment and investigation, and research. The process includes assessments of: Protection - Can be defined as the state of being defended, safeguarded, or shielded from injury, loss, or destruction from natural or unnatural forces. Vulnerability â€” The quality of being susceptible to attack or injury, warranted or unwarranted, by accident or by design. Risk â€” The possibility or likelihood of being attacked or injured. Mitigation â€” The ability to alleviate, reduce, or moderate a vulnerability, thus reducing or eliminating risk. Controversy[edit] There have been public criticisms of the mechanisms and implementation of some security initiatives and grants, with claims they are being led by the same companies who can benefit, [12] and that they are encouraging an unnecessary culture of fear. Commentators note that these initiatives started directly after the collapse of the Cold War , raising the concern that this was simply a diversion of the military-industrial complex away from a funding area which was shrinking and into a richer previously civilian arena. Grants have been distributed across the different states even though the perceived risk is not evenly spread, leading to accusations of pork barrel politics that directs money and jobs towards marginal voting areas. The Urban Areas Security Initiative grant program has been particularly controversial, with the infrastructure list covering 77, assets, including a popcorn factory and a hot dog stand. An absence of comparative risk analysis and benefits tracking it has made it difficult to counter such allegations with authority. In order to better understand this, and ultimately direct effort more productively, a Risk Management and Analysis Office was recently created in the National Protection and Programs directorate at the Department of Homeland Security. But as part of the CIP program, DoD has responsibilities that traverse both the national and department-wide critical infrastructure. PDD identified the responsibilities DoD had for critical infrastructure protection. First, DoD had to identify its own critical assets and infrastructures and provide assurance through analysis, assessment, and remediation. DoD was also responsible for identifying and monitoring the national and international infrastructure requirements of industry and other government agencies, all of which needed to be included in the protection planning. DoD

also addressed the assurance and protection of commercial assets and infrastructure services in DoD acquisitions. Other DoD responsibilities for CIP included assessing the potential impact on military operations that would result from the loss or compromise of infrastructure service. There were also requirements for monitoring DoD operations, detecting and responding to infrastructure incidents, and providing department indications and warnings as part of the national process. Ultimately, DoD was responsible for supporting national critical infrastructure protection. In response to the requirements identified in PDD, DoD categorized its own critical assets by sector, in a manner similar to the national CIP organization. The DoD identified a slightly different list of infrastructure sectors for those areas that specifically required protection by DoD. DoD sectors[edit] There are ten defense critical infrastructure sectors that are protected by the DoD. Financial Services - Defense financial services support activities related to officially appropriated funds. These activities include the disbursement of cash, receipt of funds, and acceptance of deposits for credit to officially designated Treasury general accounts. This sector also provides financial services to individuals and on-base organizations, including deposits, account maintenance, and safekeeping. These include surface, sea, and lift assets; supporting infrastructure; personnel; and related systems. Public Works - Public works includes four distinct physical infrastructure sectors: This defense infrastructure sector is composed of networks and systems, principally for the distribution of the associated commodities. The Corps of Engineers is responsible for coordinating the assurance activities of the public works infrastructure sector. The GIG is the globally interconnected set of personnel, information, and communication capabilities necessary to achieve information superiority. C2 includes assets, facilities, networks, and systems that support mission accomplishment. Intelligence Surveillance, and Reconnaissance, or ISR - The Defense Intelligence, Surveillance and Reconnaissance infrastructure sector is composed of facilities, networks, and systems that support ISR activities such as intelligence production and fusion centers. The Defense Intelligence Agency , or DIA, is responsible for coordinating the assurance activities of this infrastructure sector. Health Affairs - The health care infrastructure consists of facilities and sites worldwide. Some are located at DoD installations; however, DoD also manages a larger system of non-DoD care facilities within its health care network. These health care facilities are linked by information systems. Personnel - The defense personnel infrastructure sector includes a large number of assets hosted on component sites, a network of facilities, and information systems linking those sites and facilities. In addition to being responsible for its own assets, the personnel infrastructure sector also coordinates commercial services that support the personnel function. These services include recruitment, record keeping, and training. The Defense Human Resources Activity is the designated lead component for the Defense Personnel infrastructure sector. Space - The defense space infrastructure sector is composed of both space- and ground-based assets including launch, specialized logistics, and control systems.

Chapter 2 : National Critical Information Infrastructure Protection Centre - Wikipedia

The critical information infrastructure (CII) is [a]ny physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video that is.

Messenger This is the first article in our series Making Cities Work. It considers the problems of providing critical infrastructure and how we might produce the innovations and reforms needed to meet 21st-century needs and challenges. Our cities and regions depend on the critical nodes and arteries that together comprise urban infrastructure systems. This includes energy, food, water, sewerage and communications. The positioning of critical infrastructure is crucial to our understanding of the world we live in and how we see ourselves. This means key questions around critical infrastructure need to be better considered. How is it critical, when and for whom? Beyond espionage, sabotage and coercion Critical infrastructure has received much attention in recent years. The reasons include concerns about exposure to terrorist attack, disruption by disasters, rising awareness of the interdependent nature of urban infrastructure, and changes in ownership and responsibility for infrastructure assets. The Australian government defines critical infrastructure as: This definition expands traditional thinking to include network and information infrastructure. However, the emphasis is on national security and defence issues such as espionage, sabotage and coercion. Infrastructure is defined as critical on the basis of what is at threat should it be destroyed or disabled, and how much that matters. Yet what is critical about critical infrastructure is not just a matter of national security threats. It is also the key linkages between this infrastructure and human and environmental system vulnerability, integrity and equity. Experiences of critical infrastructure are not equal, but highly contingent on political and economic priorities, influence and opportunity. Critical how and for whom? When securing urban infrastructure, the focus is on whom or what is being secured â€" and from what. Any issue is capable of securitisation which involves casting the security issue as a threat that calls for emergency measures. But security for whom? And at what cost? Critical infrastructure can be government-owned such as dams , privately owned like airports , community-owned like irrigation systems , or involve public-private partnerships like electricity distribution networks. The ownership patterns of infrastructure of all kinds have changed rapidly in recent years. This has left questions of responsibility unresolved. An example is the ownership versus service provision arrangements for the supply and distribution of catchment water resources. Alongside the need for improved service quality, cost efficiencies, variety and choice, a growing trend towards highly uneven and inequitable community and environmental outcomes demands our attention. How critical infrastructure is defined influences which stakeholders are deemed to have a role or responsibility in protecting it. In South Australia, a severe thunderstorm blacked out the state in The resulting political finger-pointing distracted attention from the real issues of risk and responsibility in delivering electricity to the community. Critical when and at what scale? The scale question leads us to consider assets not normally included as critical infrastructure. An example is the vital role of natural ecosystems in our long-term economic and social welfare. Natural or semi-natural water catchments are in many places the sole source of water for towns and cities. An alternative to a national security approach to critical infrastructure involves a complementary focus on the local scale. Local access to food, for instance, can be seen as critical. The Australian Food Sovereignty Alliance argues for community-scale urban food policies and practices. In , foot and mouth disease broke out in the UK. That underscores the merits of social and environmental policy at local government level. Big assets and sudden events are at one level defensible as a prime focus. But this approach is limited by a traditional framing of critical infrastructure and a bias towards certain timeframes. Decisions on resources, priorities and effort inevitably involve scale-dependent judgements. These judgements should be defined by the nature of the impacts: For example, local infrastructure â€" minor roads, flood buffers, bridge culverts and so on â€" is critical for society to function. Yet it is not well catered for in policy. Local government capacity to provide and manage infrastructure is limited. And varying interpretations of scale and criticality shape the funding debate. Our urban arteries Critical infrastructure networks shape and sustain our cities and regions. But they also expose communities to a range of threats. These include natural disasters, terrorism, peak oil and climate

change. So how do we decide what is critical and what is not? How can we better recognise and integrate natural ecosystems as critical to human survival and flourishing? How do we do this amid infrastructure privatisation and securitisation? And where are the points of resistance and pathways for alternative action? We need to be more imaginative about critical urban infrastructure. A better, more sustainable approach needs to: This article draws on a research paper by the authors in a new special issue of the international journal, Urban Policy and Research, on critical urban infrastructure. You can read other published articles in our series here.

Chapter 3 : Critical information infrastructures protection (CIIP) - OECD

Critical (Information) Infrastructure is the set of computers, computer systems, telecommunication networks, data and information, the destruction or interference may weaken or impact the safety of the economy, public health, or combination thereof, in a nation.

For instance, operators of CII are required to follow special security procedures, to store certain data within mainland China, and to use a new security review process when buying network equipment or services. While revisions can be expected in response to public and industry comments, these draft regulations make clear that the reach of CII will be quite expansive. In addition to sectors previously mentioned in the Cybersecurity Law and other related measures, Chapter 3 of the new regulations names sectors such as media, specifically including radio stations, television stations, news agencies, and other such news work units. It also adds sanitation and healthcare, plus work units providing cloud computing, big data, and other such large-scale public information network services. In turn, all line ministries in the Chinese administration will be required to identify and list the CII within their portfolio, a recipe for administrative one-upmanship and rent-seeking. The rising role of standards If the new evidence about how CII will be defined clarifies some matters, the draft regulations also suggest further clarification is in store by stating that new cybersecurity standards will be used to guide the work of protecting CII. It remains unclear how many standards related to CII are being developed, but there already appear to be nearly a dozen, including some that get into more granular detail about how many users a network operator must have to be considered a CII operator. This could be important for e-commerce providers among other businesses. It is already clear, however, that major e-commerce players such as Alibaba, Tencent, and JD. They could be included, for example, as cloud services and big data providers. Laws such as the Cybersecurity Law provide broad frameworks, while regulations and measures guide implementation and add specificity, and standards provide more highly technical guidelines that may clarify otherwise murky principles. In a cross-sectoral and interlocking regime such as this, decision makers at various levels are likely to maintain significant discretion. They point out that the regulations in Article 38 call for the establishment of a cybersecurity information sharing system among the government, the private sector, and academia. The CAC headquarters and its subordinate cybersecurity and informatization departments at the provincial and more local levels are given a lead role in a range of actions and system development called for in the new regulations, such as organizing information sharing systems and conducting emergency response drills. Overlapping responsibilities and uncertainty Even as businesses face the challenges a new and changing regulatory environment, Chinese officials will face broad challenges of their own. Regulators in CII sectors are given a role in operationalizing and enforcing the regulations once they are finalized, and some sectoral regulators may prove better prepared than others. Some foreign cloud services providers, for example, have received Level 3 certification under the MLPS, and the status of these certifications remains in doubt under the new framework. Expanding scope of sovereignty and local control The draft regulations reiterate controversial data localization requirements in the Cybersecurity Law: While this seems self-evident with regard to infrastructure such as an electric grid that is fixed in place, Article 18 of the draft regulations defines CII not on the basis of location, but of ownership. The same could be said for any other CII operator. The question of whether such requirements would violate WTO disciplines may arise, but it is not so important in the short run: A case is unlikely to be brought any time soon, and even if China were to lose such a case, the effects in practice would likely be very limited. What is next for Cybersecurity Law implementation? Article 31 of the new draft regulations reiterates language in the Cybersecurity Law requiring that network products and services purchased by network operators must undergo a cybersecurity review under a new Cybersecurity Review Regimeâ€”the same new regime that may be in tension with the MPS-associated Multi-Level Protection Scheme as discussed above. The new review regime is awaiting an important next stage of implementation, including the naming of third-party review organizations that will evaluate products and the establishment of a Cybersecurity Review Committee and an associated Expert Committee, as called for in another recent regulatory document, the Interim Security Review Measures for Network Products and Services

see full translation here. The new draft regulations on CII more explicitly link the Cybersecurity Review Regime to CII operators, and potentially expand the scope of reviews further down supply chains, thereby affecting companies that may not in themselves qualify as CII.

Chapter 4 : CRITIS - The 11th International Conference on Critical Information Infrastructures Security

Critical Information Infrastructures also include the things listed above, which are in the possession or under the control of the State (national, provincial or local), and anyone exercising a public power or performing a public function.

Chapter 5 : Chinaâ€™s Ambitious Rules to Secure â€˜Critical Information Infrastructureâ€™

This information-protection program enhances information sharing between the private sector and the government. Protected information can be used to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures.

Chapter 6 : Altmetric â€“ Critical Information Infrastructure Security

critical infrastructures as well as new forms of communication, information exchange and commerce. This symbiosis is a national security priority, since the information.

Chapter 7 : Critical Information Infrastructure - CIPedia

Methodologies for the identification of Critical Information Infrastructure assets and services The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe.

Chapter 8 : Critical Information Infrastructures â€” ENISA

Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety.

Chapter 9 : Critical infrastructure protection - Wikipedia

Critical infrastructure protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.