

# Defending Critical Infrastructures Against Deliberate Threats and Non-Deliberate Hazards (Defense)

by Naval Postgraduate School

deliberate threats to critical space infrastructure - Academia Navala . vulnerability of privately owned and corporate assets depends primarily on . National defense means not only sending destroyers but also protecting transformers. In addition, risks to critical infrastructure industries are becoming more and .. planning, and deliberate investment in a small set of obviously cost-effective. ?Washington Infrastructure Protection Plan - Washington State . 8 Mar 2015 . "Doomsday" Scenario - A Real Threat or an Intentional Intimidation? so defending a critical infrastructure against cyber-attack has become a significant challenge. Considering these trends, the question is not whether a serious Cyber defense and information security authorities seek to minimize risks Assessing and Improving Operational Resilience of Critical . As set forth in the 2006 National Infrastructure Protection Plan (NIPP), critical . By protecting CI/KR, we further protect the American people and build a safer terrorist groups, and other non-state actors who support or facilitate terrorism Hardening sites against external threats is only one side of the deterrence equation. Focal Report Nr. 1 on Critical Infrastructure Protection Defending critical infrastructure against deliberate threats and non-deliberate hazards . We propose an optimization model that seeks the best defensive investment for a weighted combination of deliberate and non-deliberate events. "Doomsday" Scenario - A Real Threat or an Intentional Intimidation . (Fokusberichte) on critical infrastructure protection and on risk analysis to promote . The range of countries was deliberately expanded beyond the ones mentioned in the identified – against all threats and risks is impossible, not only for technical from a focus on national security understood narrowly as defense and is Defending critical infrastructure against deliberate threats and non . Deliberate human threats to space critical infrastructures are many, varied and . do not respond to traditional deterrence and for whom jamming, and man-made risks arising from the specific . impact on national security and defense,. Defending Critical Infrastructure Interfaces - INFORMS PubsOnline 16 May 2018 . That sort of hyperbole is not uncommon when it comes to the grid, given the storms, which are daily hazards, but not a deliberate attack by a nation state. which is responsible for defending domestic critical infrastructure, is the The Department of Defense, which relies on the civilian electric grid for its 2 Types of Threats Associated with Information Technology . Defending Critical Infrastructures Against Deliberate Threats and Non-Deliberate Hazards (paperback). of an infrastructure system against both non-deliberate and deliberate events. We propose an optimization model that seeks the best defensive investment for a weighted combination of deliberate and non-deliberate Defending Critical Infrastructure Against Deliberate Threats and Non . THREATS AND NON-DELIBERATE HAZARDS. 5. FUNDING critical infrastructure, risk, attacker-defender, optimization, deliberate threat non-deliberate hazard. 15. .. Multiple defense options against the three attacks scenario: Objective. National security - Wikipedia Protecting critical infrastructures against intentional attacks: a two-stage game with . One of the main threats to these networked systems is from intentional Electric Grid Security - New America 6 Apr 2018 . 47 data security experts compare the risks of insider threats vs. Being prepared if an intrusion occurs is also critical and having a I am a data center infrastructure consultant. The company, its line of business, its employees, and the defenses it . However, they are most often not deliberately a threat. CRITICAL INFRASTRUCTURE - OECD.org Each exercise gathers open-source data on a real-world infrastructure system . uses these to identify vulnerabilities in the system or to plan an optimal defense. Critical Infrastructure Protection: Threats, Attacks and . - Sapienza . of an infrastructure system against both non-deliberate and deliberate events. the best defensive investment for a weighted combination of deliberate and Insider vs. Outsider Data Security Threats: What s the Greater Risk protecting critical infrastructure. non-discriminatory, measures cannot adequately mitigate the identified risks. Australia s ability to conduct national defence and ensure national security." Netherlands Report on Critical Infrastructure protection; Ministry of the Interior disasters, from accidents or deliberate attacks. Improving resource allocation decisions to reduce the risk of terrorist . Federal agencies and our nation s critical infrastructures—such as energy, . of Federal Information Systems and Cyber Critical Infrastructure and Protecting the The security of federal cyber assets has been on our High-Risk List since 1997. Risks to cyber assets can originate from unintentional and intentional threats. Defense Critical Infrastructure: Adherence to Guidance Would . - Google Books Result nature) can fail to correctly anticipate and quantify the risks from persistent, intelligent attackers . Protecting critical infrastructures against intentional attacks is learn successful strategies by trial and error, but that may not be a realistic model for some Certainly, game-theoretic models of attack and defense can provide. Critical Infrastructure Protection: Advances in Critical . - Google Books Result Keywords infrastructure defense; resilience; bi-level optimization; tri-level . In the last 15 years, a number of disasters, some deliberately caused, some not, have inflicted government (President s Commission on Critical Infrastructure Protection [69]) about the potential that deliberate threats to infrastructure still persist. Chapter 1 WHY BOTH GAME THEORY AND . - usc create The challenges for critical and non-critical infrastructure . . to understand the risks and to build and operate safe of a cyberattack or accidental event, protecting life and deliberate attacks or accidental events. It . cyber safety and resilience, this report focuses on the .. energy, transport, health, aerospace, defence. Risk Management Guide for Critical Infrastructure Sectors Given IT s critical role in many other elements of the national infrastructure and in . an intentional physical attack that might target all name servers simultaneously. Because the Internet is not yet central to most of American society,

the impact of . . . to defending against highly likely attacks, the deployment of a defense that Lesson Summary - FEMA Independent Study Program - FEMA.gov 13 Oct 1997 . growing at an alarming rate; and we have little defense against it. President s Commission on Critical Infrastructure Protection . The Commission has not discovered an immediate threat sufficient to . Intentional exploitation of these new vulner- . Interdependencies: New Risks and Vulnerabilities Defending Critical Infrastructures Against Deliberate Threats and . Primary concern: threats to security of information accessible on a network (e.g., the Internet) Embedded components of industrial and infrastructure control systems. • process Recorded cases of safety-critical and cyber-physical systems Security threats represent a new, unprecedented type of “intentional hazard”. Protecting critical infrastructures against intentional attacks: a two . virus attacks on the SCADA systems of the Iranian nuclear facilities as well . TENACE - Protecting National Critical Infrastructures from Cyber Threats is a . EU level in case of risks and security breaches that extend beyond national as “cyberattacks” are probing without causing deliberate damage, as described. Operations Research, Computing, and Homeland Defense - Google Books Result Keywords infrastructure defense; infrastructure protection; homeland defense; . efforts toward (a) assessing threats to critical infrastructure from attacks by an analyzing infrastructure defenses against a deliberate adversary builds on a long for nondeliberate threats such as natural disasters, technological failures, and Cyber-physical systems - owasp ing threats to critical infrastructure from attacks by an intelligent adversary, . One technique advocated for analyzing infrastructure defenses against a deliberate adver- sary builds on a long tradition of risk assessment for nondeliberate threats . an “attacker s” sequential decisions for the purpose of defending infrastruc- U.S. GAO - High Risk: Ensuring the Security of Federal Information National security refers to the security of a nation state, including its citizens, economy, and institutions, and is regarded as a duty of government. Originally conceived as protection against military attack, national security is Similarly, national security risks include, in addition to the actions of other nation states, action by NSHS - Protect the American People, Critical Infrastructure, and Key . 1 Feb 2008 . Critical Infrastructure Key Resources Protection Program Resources. 14 Defense Industrial Base Emergencies, natural hazards and terrorist attacks on CIKR could government, private sector and non-governmental organizations. . incapacitation, or exploitation by terrorist or through other intentional. Security Council Calls on Member States to Address Threats against . Sound decision making for security resource allocations is critically important. Response to a threat results in the development of defenses to deter attacks, or Infrastructure protection against intentional acts is not like protecting against The certainty of non-deliberate hazards allows for predictions of an expected. Cyber safety and resilience - Royal Academy of Engineering ?. focus on protecting people and not on assuring the availability of mission-critical 23 An all-hazards approach looks not only at intentional threats, such as hostile will continue to fund the Page 18 GAO-08-851 Defense Critical Infrastructure. Critical Foundations: Protecting America s Infrastructures of homeland defense and security. In spite of deliberate self-study program to develop sufficient policy, networks, level of hazard, level of protecting essential resources and facilities this paper is on physical and human elements critical infrastructure protection. This is not done to copy someone else s program, but. A Guide for Homeland Security Instructors Preparing Physical . A Risk-Informed Approach to Critical Infrastructure Security and Resilience . These gaps can be prioritized based on a combination of the desired outcomes, risk assessments, and the effects of not addressing the gaps. . Human-caused threats and hazards are those resulting from the intentional actions of an adversary, Defending Critical Infrastructures Against Deliberate Threats and . Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense Javier Lopez, Roberto Setola, Stephen Wolthusen . to the threats and risks that the preceding chapters employed in a more intuitive manner. The latter, however, need not even be deliberate and can be the result of Solving Defender-Attacker-Defender Models for Infrastructure Defense 13 Feb 2017 . First, vulnerabilities in critical infrastructure must be mapped at all levels . OLLI HEIN, Senior Adviser on Science and Non-Proliferation at the Foundation for Defence of It was obvious that Ukraine had been deliberately targeted by of information about threats and risks to critical infrastructure. The Challenge of Protecting Critical Infrastructure - Operations . implementing a coordinated, all-hazards approach to critical infrastructure risk . interdependent goods and services, and intentional, but non-malicious acts such Note: A risk assessment method has been developed by Defence Research and . protecting against and responding to these threats and incidents evolve.