Towards an Information Asset-Based Defensive Cyber Damage Assessment Process
MR Grimaila, LW Fortson - Computational Intelligence in …, 2007 - ieeexplore.ieee.org

... While the need for effective cyber damage assessment was recognized more than a decade ago, little progress has been made to attain this objective. However, the explosive growth of cyber attacks on military networks and the dependency on cyberspace to conduct ...

Cited by 16 Related articles

Unifying strategies and tactics: a survivability framework for countering cyber attacks
Y Zuo, B Panda - Intelligence and Security Informatics, 2009. ISI …, 2009 - ieeexplore.ieee.org

... transmission of local status and observational data, synthesis of incoming data for the regional ... assume that during wartime, the enemies have launched a series of cyber attacks targeting ... communications; and (2) trying to obtain intelligent information about the military force and ...

Cited by 4 Related articles

Coping with Uncertainty: Command and Control in Information Degraded Environments
MW Kessler - 2010 - DTIC Document

... security firms revealed the interface between crime and espionage in the cyber domain. 33 ... information assurance across the range of military operations while sustaining effectiveness. ... game, these principles also should be part of on-going training for the serving operational ...

Cited by 1 Related articles

DoD Global Information Grid Mission Assurance
A Bargar - 2008 - DTIC Document

... To better understand the shortfalls and enable solutions, DoD priorities in this area include the following: • Exercising military operations under a severely degraded cyber environ- ment. • Improving resilience, prioritization for recovery, and continuity of operations. ...

Cited by 4 Related articles

[PDF] Ten Propositions regarding Cyberspace Operations
BT Williams - Joint Force Quarterly, 2011 - ndu.edu

... Yet our defenses for the most part are equally distributed across the entire nonclassified ... The US military must be prepared to engage a variety of adversaries. ... Unfortunately, no commander can create an impregnable cyber defense and still execute operational command and ...

Cited by 2 Related articles

Cyberspace and the Operational Commander
GL Tritz - 2010 - DTIC Document

... The US already incorporates cyberspace for command and control and Information ... achieve military objectives. ... Bradley L. Boyd, “Cyber Warfare: Armageddon in a Teacup?” (master's thesis, Fort Leavenworth, KS: US Army Command and General Staff College, 12 November ...

Cited by 1 Related articles

Improving the cyber incident mission impact assessment (CIMIA) process
MR Grimaila, RF Mills, LW Fortson - … of the 4th annual workshop on Cyber …, 2008 - dl.acm.org

... This presentation will review of the importance of accurate and timely damage assessment in military operations; motivate the need for a ... 4, No ... Taddaa, G., J. Salerno, D. Boulware, M. Hinman, & S. Gorton, “Realizing Situation Awareness in a Cyber Environment,” Proceedings of ...

Cited by 5 Related articles

[PDF] Defending warfighter networks
A Ghosh - 2005 - archive.darpa.mil

... The initial groundwork for self-defending networks has been laid by two ongoing DARPA projects,
Dynamic Quarantine of Computer-Based Worms and Defense Against Cyber Attacks on the MANET ... The DoD vision for the GIG and future military operations requires all DoD ...

Cited by 2 Related articles

On Cyber Warfare Command and Control Systems
NR Howes, M Mezzino, J Sarkesain - 2004 - DTIC Document
... Military commanders know that there are times when the best defensive strategy is to take the ... al, Cyber Warfare Command and Control System Users Manual, Draft IDA document, July 2003. ...
Cited by 4 Related articles

Air Force Cyber Command (Provisional) Decision Support
R Mesic, M Hura, MC Libicki, AM Packard, LM Scott - 2010 - DTIC Document
... operational preparation of the environment in coordination with the Global Command and Control System; executing ... However, in emerging constructs for cyber and IO organizations, the medium and ... overt or covert actions with or without more-conventional military action at the ...
Cited by 3 Related articles

Cyber situation awareness as distributed socio-cognitive work
M Tyworth, NA Giacobe, V Mancuso - Proc. of SPIE Vol, 2012 - spiedigitallibrary.org
... interviews we conducted ethnographic observations of the United States Military Academy participating ... 14] N. Giacobe and S. Xu, "Geovisual Analytics for Cyber Security: Adopting ...
Quantitative Methods: Triangulation in Action," Administrative Science Quarterly, 24(4), 602 (1979 ...
Cited by 1 Related articles

BL Hale - 2010 - DTIC Document
... infrastructures are not defined, the association of both physical and cyber infrastructures essential to planning and executing military operations is contained within the definition ... cyber assets that must be secured for the achievement of certain mission-critical tasks. ...
Cited by 5 Related articles

CAMUS: automatically mapping cyber assets to missions and users
JR Goodall, A D'Amico... - ... , 2009. MILCOM 2009. ..., 2009 - ieeexplore.ieee.org
Abstract This research advances Cyber Situation Management by proposing methods for automated mapping of Cyber Assets to Missions and Users (Camus). To enable accurate and efficient cyber incident mission impact assessment, a Camus

Generated by Google Scholar Citation Explorer
http://combio.cs.uic.edu/~mayank/software/slh/
Abstract: Virtually all organizations have embedded information and communication technologies into their core organizational processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize profit. ...

Related articles

CAMUS: Automatically Mapping Cyber Assets to Mission and Users (PREPRINT)
JK Kopylec, JR Goodall - 2009 - DTIC Document
Abstract: This research advances Cyber Situation Management by proposing methods for automated mapping of Cyber Assets to Missions and Users (CAMUS). To enable accurate and efficient cyber incident mission impact assessment, a CAMUS ontology that defines ...

Related articles

C Peterson, MR Grimaila, R Mills, MW Haas, G Thomas… - world-comp.org
Information is a critical asset on which all modern organizations depend to meet their mission objectives. Military organizations, in particular, have embedded Information and Communications Technologies (ICT) into their core mission processes as a means to...

Related articles

[PDF] A Survey of Cyberspace Mission Assurance within United States Air Force Communications Squadrons
M Evans, MR Grimaila, RF Mills - elron.informatik.tu-freiberg.de
Abstract—The United States Air Force (USAF), like many other large enterprises, has embedded information and communication technologies into their core organizational processes as a means to increase operational efficiency, improve decision making quality, ...
Related articles

D Sorrels, MR Grimaila, LW Fortson, RF Mills - ... and Security (ICIW 2008), Peter Kiewit ..., 2008
Cited by 6 Related articles

C Peterson - 2011 - DTIC Document
Abstract: Information is a critical asset on which virtually all modern organizations depend upon to meet their operational mission objectives. Military organizations, in particular, have embedded Information and Communications Technologies (ICT) into their core mission ...
Related articles

Mission Assurance Analysis of Theater Ballistic Missile Defense Systems
Abstract: In today's budget-constrained environment with aging equipment and rapid technology turnover, the commander's requirement to prioritize and justify funding requests has essentially become an exercise in mission assurance. This study addresses the...

Design considerations for a cyber incident mission impact assessment (CIMIA) process
Abstract: Virtually all modern organizations have embedded information systems and networking technologies into their core business processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize ...
Cited by 15 Related articles

An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment
MR Grimaila, RF Mills, LW Fortson - 2008 - DTIC Document
Abstract: The use of information technologies to enhance Command and Control (C2) processes has yielded enormous benefits in military operations. Commanders are able to make higher quality decisions by accessing multiple information resources; obtaining ...
Cited by 10 Related articles

[PDF] Developing methods for timely and relevant mission impact estimation
MR Grimaila, LW Fortson Jr, JL Sutton... - SPIE Defense, Security, ..., 2009 - 144.206.159.178
ABSTRACT Military organizations embed information systems and networking technologies into their core mission processes as
a means to increase operational efficiency, improve decision making quality, and shorten the "kill chain". Unfortunately, this dependence can...

Cited by 7 Related articles

**A scalable architecture for improving the timeliness and relevance of cyber incident notifications**
JL Miller, RF Mills, MR Grimaila... - Intelligence in Cyber ..., 2011 - ieeeexplore.ieee.org

Abstract The current mechanics of cyber incident notification within the United States Air Force rely on a broadcast “push” of incident information to the affected community of interest. This process is largely ineffective because when the notification arrives at each unit, ...

Cited by 1 Related articles

**Integration of Cyber Situational Awareness into System Design and Development**
LE Chase - 2009 - DTIC Document

Abstract: Cyber situational awareness (SA) is the correlation of network status to operational impact. This capability is increasingly important for commanders and individual weapon system platforms as the DoD continues its exploitation of net-centric operations. To ...

Related articles

**Computing the impact of cyber attacks on complex missions**
S Musman, M Tanner, A Temin... - (SysCon), 2011 IEEE ..., 2011 - ieeeexplore.ieee.org

Abstract This paper describes how to evaluate the impact of a cyber attack on a mission. We accomplish this by computing impact as the changes to mission measures of effectiveness, based on the reported effects of a known or suspected attack on one or more parts of the...
An hierarchical asset valuation method for information security risk analysis
U Tatar, B Karabacak - Information Society (i-Society), 2012 ...
Abstract: The widespread use of information technology transforms businesses continuously and rapidly. Information technology introduces new threats to organizations as well. Risk analysis is an important tool in order to make correct decisions and to deal with cyber ...

A framework of survivability requirement specification for critical information systems
Y Zuo - System Sciences (HICSS), 2010 43rd Hawaii ...
Abstract: Survivability represents a system's ability to provide essential services in the presence of attacks and failures, and to recover full services in a timely manner when the environment improves. For many critical systems used in national defense, healthcare, ...

Models of Quality of Service and Quality of Information Assurance Towards Their Dynamic Adaptation
N Ye - 2011 - DTIC Document
Abstract: This report documents the details of the technical work accomplished by Arizona State University on defining Quality of Service (QoS) and Quality of Information Assurance (QoIA) models/metrics to enable intelligent QoS and QoIA trade-offs. ASU's task was to: (1) ...

A Survivability Analysis Framework of Command Automation System
Abstract The reinforced security strategy can't ensure the survivability of command automation system under information warfare. To solve non-standardized and non-practical problems of present survivability analysis, a practical and operational survivability ...

Related articles

[PDF] Tradeoffs of Service, Security and Attack for Cyber System Survivability
N Ye, BM Aranda - dpse.eas.asu.edu
Abstract—Tradeoffs within the limitation of given system resources often have to be made for a cyber system to sustain its more critical services under the damage of cyber attacks. Understanding and modeling cause-effect dynamics of activities (service, security and ... Related articles

Improving the cyber incident mission impact assessment (CIMIA) process
MR Grimaia, RF Mills, LW Fortson - ... of the 4th annual workshop on ..., 2008 - dl.acm.org
Abstract Despite our best efforts to secure our cyberspace; we inevitably experience incidents in the cyber domain which result in the loss of the confidentiality, integrity, or availability of a cyber resource. When a cyber incident occurs, we must quickly and ... Cited by 5 Related articles

[PDF] Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels
D Bodeau, R Graubart... - Proceedings of the 2010 ..., 2009 - wwwsrv1.mitre.org
Executive Summary The MITRE-developed cyber preparedness
(Cyber Prep) framework provides an approach for addressing the cyber threats that an organization or mission faces; determining the level of preparedness necessary to ensure mission success; facilitating ...

Cited by 3 Related articles

An Architecture for Improving Timeliness and Relevance of Cyber Incident Notifications
J Miller - 2011 - DTIC Document
Abstract: This research proposes a communications architecture to deliver timely and relevant cyber incident notifications to dependent mission stakeholders. This architecture, modeled in Unified Modeling Language (UML), eschews the traditional method of pushing ...

Cited by 2 Related articles

On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy
R Belk, M Noyes - 2012 - DTIC Document
Abstract: Analysis and policy recommendations for use and response to various forms of cyber action for Offensive Military Cyber Policy. Establishes a pragmatic policy-relevant, effects-based ontology for categorizing cyber capabilities. Develops a comprehensive ...

Related articles

[PDF] On the Use of Offensive Cyber Capabilities
R Belk, M Noyes - 2012 - live.belfercenter.org
Abstract: Analysis and policy recommendations for use and response to various forms of cyber action for Offensive Military Cyber Policy. Establishes a pragmatic policy-relevant, effects-based ontology for categorizing cyber capabilities. Develops a comprehensive ...

Related articles
USCYBERCOM: A Centralized Command of Cyberspace
SM Rodriguez - 2011 - DTIC Document
Abstract: The unprecedented growth of cyberspace and related technologies has impacted nearly every aspect of human society and has opened a new domain in which information is communicated more rapidly than ever before. Recognizing the growing potential of...
Related articles

[PDF] A systematic comprehensive computational model for stake estimation in mission assurance
RK Abercrombie, FT Sheldon... - ... Conference on Social ..., 2010 - info.ornl.gov
Abstract—In earlier works, we presented a computational infrastructure that allows an analyst to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. In this paper, we discuss how this ...
Cited by 3 Related articles

Methodology for evaluating security controls based on key performance indicators and stakeholder mission
FT Sheldon, RK Abercrombie... - System Sciences, 2009. ..., 2009 - ieeexplore.ieee.org
Abstract Information security continues to evolve in response to disruptive changes with a persistent focus on information-centric controls and a healthy debate about balancing endpoint and network protection, with a goal of improved enterprise/business risk ...
Cited by 13 Related articles

Assessing operational impact in enterprise systems with dependency discovery and usage mining
A framework for monitoring the dependencies between users, applications, and other system components, combined with the actual access times and frequencies, was proposed. Operating system commands were used to extract event information from the end-user ...

Related articles

An approach to the automated determination of host information value
JM Beaver, RM Patton, TE Potok - Computational Intelligence in ..., 2011 - ieeexplore.ieee.org
Abstract: Enterprise networks are comprised of thousands of interconnected computer hosts, each of which is capable of creating, removing, and exchanging data according to the needs of their users. Thus, the distribution of high-value, sensitive, and proprietary information ...
Related articles

Connecting the edge: mobile ad-hoc networks (manets) for network centric warfare
BA Peacock - 2007 - DTIC
Abstract: The principles of Network Centric Warfare (NCW) are at the heart of DoD transformation plans and are the driving concept of several high profile acquisition programs. This paper addresses the question of what communications and networking ...
Cited by 4 Related articles

A good IDS response protocol of MANET containment strategies
BC Cheng, C Huan, RY Tseng - IEICE transactions on ..., 2008 - search.ieice.org
Much recent research concentrates on designing an Intrusion Detection
A Legal Reasoning Component of a Network Security Command and Control System
G Dementis, G Sousa - 2010 - DTIC Document
Abstract: There are numerous computer-aided tools to enable Computer Network Defense. However, their effectiveness in countering attacks is less than optimal when they are used independently of one another. Research has identified the requirements for an integrated ...
Cited by 3 Related articles

[PDF] Forensics, Fighter Pilots and the OODA Loop: The role of digital forensics in cyber command and control
HMB Dussault, CJ Maciag - Digital Forensic Research Workshop, 2004 - dfraws.org
Abstract Derived from personal observations of the differences between winning a losing a dogfight, the ability rapidly move through a decision cycle of observing, orienting, deciding and acting (ie, Boyd's OODA loop) is a central concept in modern military command and ...
Cited by 2 Related articles

A legal reasoning component of a network security command and control system
G Sousa - 2010 - calhoun.nps.edu
There are numerous computer-aided tools to enable Computer Network Defense. However, their effectiveness in countering attacks is less than optimal when they are used independently of one another.
Research has identified the requirements for an integrated ... 

Related articles

[PDF] A Theory of Distributed Systems
NR Howes - Citeseer
Abstract The theory $\theta$ presented here is the smallest theory in the temporal logic TLB [10] that all distributed systems, according to our definition of a distributed system, must satisfy. $\theta$ is an instance of the classical modal logic S4. 2. The central theorems of $\theta$ are stated here ...

Related articles

CYBER COMMAND
JL Samaan - The RUSI Journal, 2010 - Taylor & Francis
Abstract US efforts to develop a coherent cyber-strategy have foundered because of a fundamental divide in the interpretation of the conduct of cyber-warfare. Yet both sides of this intellectual rift could be in the wrong. As such, cyberspace does not lend itself to analogies ...

Cited by 1 Related articles

[PDF] The American and Russian Approaches to Cyber Challenges
D Fayutkin - J Def Manag, 2012 - omicsgroup.org
Abstract Cyber warfare presents new challenges to western governments and private organizations. The gravest danger posed on western governments is a strategic threat on their central information infrastructure, which necessitates the development of new ...

Related articles

[HTML] The American and Russian Approaches to Cyber Challenges
Abstract Cyber warfare presents new challenges to western governments and private
organizations. The gravest danger posed on western governments is a strategic threat on their central information infrastructure, which necessitates the development of new ...

Related articles

[PDF] Poster: Is a Picture Worth a Thousand Alerts?
NA Giacobe - cups.cs.cmu.edu
This poster presents preliminary work in the adoption of a geovisual analytic toolkit for the purpose of representing organization-level cyber security data. This data is generally represented in text form and static visualizations such as histograms and simple pie, line ...

Related articles

"Network-Enabled" and "Leader-Centric" Command and Control (C2): The Dangers of Digital Decision Making
RR McCaskill - 2011 - DTIC Document
Abstract: The DOD has grown increasingly reliant on information technologies (IT) that enable network-enabled command and control (NEC2). Evolving network-centric strategy documents focus too narrowly on improving the technological capabilities of existing C2 ...

Related articles