# principles of information security 4th edition whitman File PDF

**principles of information security 4th edition whitman** is a comprehensive textbook that has become a foundational resource for students, practitioners, and educators in the field of information security. Authored by Whitman and Mattord, this edition continues to build on the principles established in previous versions, offering in-depth insights into the core concepts, practices, and evolving challenges of protecting information assets in an increasingly digital world. With a focus on both theoretical foundations and practical applications, the book emphasizes the importance of a holistic approach to security that encompasses policies, technology, and human factors. This article explores the key principles outlined in the 4th edition of Whitman?s book, providing an overview of the essential concepts that underpin effective information security management.

## Overview of Principles of Information Security

The principles of information security serve as the backbone for designing, implementing, and maintaining secure systems and environments. Whitman?s 4th edition underscores that these principles are not static; they evolve alongside technological advancements, emerging threats, and changing organizational needs. The book emphasizes that understanding and applying these core principles is vital for establishing a resilient security posture.

The primary goal of information security, as outlined in the book, is to protect the confidentiality, integrity, and availability (CIA) of information. These three pillars form the foundation upon which all security policies and practices are built. A thorough grasp of these concepts enables organizations to develop effective strategies for safeguarding their data and systems.

## Core Principles of Information Security

The 4th edition of Whitman?s book distills the complex field of information security into several core principles that guide best practices and decision-making processes.

### 1. Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals or systems. Maintaining confidentiality involves implementing controls such as encryption, access controls, and secure authentication methods. Whitman highlights that breaches of confidentiality can lead to data leaks, privacy violations, and loss of trust.

Key practices for maintaining confidentiality include:

- Encryption of data at rest and in transit
- Strong authentication mechanisms
- Role-based access control (RBAC)
- Regular audits and monitoring

### 2. Integrity

Integrity involves safeguarding the accuracy and completeness of information. It ensures that data is not altered, tampered with, or destroyed maliciously or accidentally. Whitman stresses that integrity controls are essential for maintaining trust in the data used for decision-making.

Common integrity measures include:

- Hash functions and checksums
- Digital signatures
- Version control systems
- Audit trails

### 3. Availability

Availability guarantees that information and resources are accessible to authorized users when needed. This principle emphasizes designing resilient systems that can withstand failures or attacks.

Strategies to ensure availability include:

- Redundancy and failover systems
- Regular data backups
- Disaster recovery plans
- Protection against Denial of Service (DoS) attacks

## Additional Principles Discussed in Whitman?s 4th Edition

Beyond the core CIA triad, Whitman?s book explores other principles that are critical for a comprehensive security framework.

### 4. Non-repudiation

Non-repudiation ensures that a party cannot deny the authenticity of their actions or communications. This is especially important in legal and contractual contexts.

Implementation techniques include:

- Digital signatures
- Secure audit logs
- Timestamping mechanisms

### 5. Accountability

Accountability involves tracking actions within a system to assign responsibility. It promotes responsible behavior and facilitates investigations in case of security incidents.

Methods to enforce accountability:

- Comprehensive logging
- User activity monitoring
- Access controls and permissions

### 6. Privacy

Privacy concerns the appropriate use and protection of personal information. Whitman emphasizes that security measures must align with legal and ethical standards to safeguard individual privacy rights.

Privacy-enhancing practices include:

- Data minimization
- Consent management
- Secure handling and disposal of data

## Applying Principles of Information Security in Practice

The principles outlined by Whitman serve as guidelines for designing security architectures, policies, and procedures. Practical application involves integrating these principles into every aspect of organizational operations.

### Developing Security Policies

Organizations should craft clear, comprehensive policies that reflect the core principles of confidentiality, integrity, and availability. Policies must be regularly reviewed and updated to address new threats and technological changes.

### Implementing Technical Controls

Technical controls such as firewalls, intrusion detection systems, encryption, and multi-factor authentication are essential tools for enforcing security principles.

### Fostering a Security-Aware Culture

Human factors play a significant role in security. Training employees, promoting security awareness, and establishing a culture of responsibility are vital for minimizing insider threats and human errors.

## Challenges and Evolving Principles

The 4th edition of Whitman?s book acknowledges that the landscape of information security is constantly evolving. New challenges such as cloud computing, Internet of Things (IoT), and sophisticated cyber attacks require continuous adaptation of security principles.

Emerging considerations include:

- Securing distributed and decentralized systems
- Managing the security risks of third-party vendors
- Balancing security with user privacy and usability

The principles of information security must be flexible yet robust enough to adapt to these changes, ensuring organizations remain resilient against threats.

## Conclusion

In summary, the principles of information security as detailed in the 4th edition of Whitman?s book provide a solid foundation for understanding and implementing effective security measures. By focusing on confidentiality, integrity, and availability, complemented by principles like non-repudiation, accountability, and privacy, organizations can develop a comprehensive security strategy. As technology advances and threats evolve, maintaining a clear grasp of these core principles is essential for safeguarding digital assets and fostering trust in information systems. Whitman?s work remains a vital resource for those committed to mastering the principles that

underpin a secure information environment.

Principles of Information Security 4th Edition Whitman: An In-Depth Exploration of Foundational Concepts

In today?s interconnected world, information security has become a cornerstone of both organizational integrity and individual privacy. As cyber threats evolve in sophistication and volume, understanding the fundamental principles that underpin secure systems is more critical than ever. Enter Principles of Information Security 4th Edition Whitman, a comprehensive textbook that has cemented itself as a vital resource for students, professionals, and anyone interested in the science of protecting digital assets. This article delves into the core concepts outlined in this authoritative work, dissecting its principles and exploring their relevance in contemporary cybersecurity landscapes.

Overview of Principles of Information Security 4th Edition Whitman

Authored by Michael E. Whitman and Herbert J. Mattord, Principles of Information Security stands as a foundational text that bridges theoretical concepts with practical applications. The fourth edition, in particular, emphasizes evolving security challenges, technological advancements, and the importance of a proactive security posture. The book?s structured approach provides readers with a deep understanding of security principles, risk management, policies, and the technical measures necessary to safeguard information assets.

Core Principles of Information Security

At its essence, information security is founded on a set of core principles that guide the development and implementation of security policies and controls. These principles serve as the compass for organizations seeking to mitigate risks and protect their resources effectively.

- Confidentiality

Definition and Importance

Confidentiality ensures that sensitive information is accessible only to authorized individuals or systems. It prevents unauthorized disclosure, whether intentional or accidental, safeguarding personal data, trade secrets, and strategic information.

Implementation Strategies

- Encryption of data at rest and in transit
- Access controls such as role-based permissions
- Authentication mechanisms like passwords, biometrics, or multi-factor authentication
- Data masking and anonymization techniques

Challenges

Balancing confidentiality with usability can be complex. Overly restrictive measures may hinder legitimate access, while lax controls increase vulnerability.

- Integrity

Definition and Significance

Integrity pertains to maintaining the accuracy, consistency, and trustworthiness of data over its lifecycle. It prevents unauthorized modifications, ensuring that information remains reliable for decision-making.

Implementation Strategies

- Checksums and hash functions to verify data integrity
- Digital signatures for authentication and non-repudiation
- Version control systems
- Access controls that restrict data modification to authorized users

Challenges

Ensuring data integrity in distributed or cloud environments can be complex, requiring robust validation mechanisms.

- Availability

Definition and Role

Availability guarantees that information and resources are accessible when needed. It supports business continuity and operational efficiency by minimizing downtime and disruptions.

Implementation Strategies

- Redundant systems and failover mechanisms
- Regular backups and disaster recovery planning
- Network security measures like DDoS mitigation
- Maintenance of hardware and software to prevent failures

Challenges

Balancing security with accessibility is vital; overly aggressive security controls may inadvertently hinder legitimate access, affecting availability.

Fundamental Security Concepts Explored in Whitman?s Textbook

Principles of Information Security emphasizes not only these core principles but also explores related concepts that form the foundation of a comprehensive security strategy.

Risk Management

Definition and Importance

Risk management involves identifying, assessing, and mitigating risks to information assets. It recognizes that no system can be perfectly secure, and prioritizes resources based on threat levels and potential impact.

Key Processes

- Asset identification and valuation
- Threat and vulnerability assessment
- Implementing safeguards proportionate to risks
- Continuous monitoring and reassessment

Frameworks and Standards

Whitman discusses various frameworks like ISO/IEC 27001, NIST Cybersecurity Framework, and COBIT, which provide structured approaches to managing security risks.

Security Policies and Procedures

Role and Significance

Policies define the organization's security posture, establishing rules and responsibilities.

Procedures translate policies into actionable steps, ensuring consistency and compliance.

Development Principles

- Clarity and specificity
- Alignment with organizational goals
- Flexibility to adapt to emerging threats
- Regular review and updates

Implementation Challenges

Ensuring organization-wide adherence requires training, awareness programs, and enforcement mechanisms.

Defense in Depth

Concept and Rationale

Defense in depth involves deploying multiple layers of security controls to protect information assets. If one control fails, others remain to provide protection.

Layers of Defense

- Physical security (locks, surveillance)
- Network security (firewalls, intrusion detection)
- Endpoint security (antivirus, patch management)
- Application security (input validation, secure coding)
- User training and awareness

Benefits

Reduces the likelihood of a successful attack and limits damage if an intrusion occurs.

Technical Controls and Countermeasures

Principles of Information Security details various technical controls that operationalize security principles.

Access Control Mechanisms

- Discretionary Access Control (DAC): Permissions assigned at the discretion of data owners
- Mandatory Access Control (MAC): System-enforced policies often used in high-security environments
- Role-Based Access Control (RBAC): Permissions assigned based on user roles

Cryptography

- Symmetric encryption for fast, bulk data protection
- Asymmetric encryption for secure key exchange and digital signatures
- Public Key Infrastructure (PKI) for managing digital certificates

Monitoring and Detection

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Security Information and Event Management (SIEM) tools
- Continuous vulnerability assessments

Organizational and Human Factors

The human element remains a critical factor in information security. Whitman emphasizes that technological measures alone are insufficient without proper organizational policies and user awareness.

User Education and Training

Regular training programs to recognize threats like phishing, social engineering, and malware.

Incident Response and Management

Establishing clear procedures for detecting, responding to, and recovering from security incidents.

Security Culture

Fostering an organizational environment where security is a shared responsibility.

Emerging Trends and Future Directions

Principles of Information Security 4th Edition Whitman also touches on emerging trends shaping the future of cybersecurity.

- Cloud Security: Addressing unique challenges posed by cloud environments, such as data sovereignty and shared responsibility models.
- Internet of Things (IoT): Securing interconnected devices with limited security controls.
- Artificial Intelligence (AI) and Machine Learning: Enhancing threat detection but also presenting new attack vectors.
- Zero Trust Architecture: Moving away from perimeter-based security to continuous verification.

Conclusion

Principles of Information Security 4th Edition Whitman offers a thorough foundation for understanding the multifaceted nature of information security. Its emphasis on the core principles?confidentiality, integrity, and availability?provides a clear framework for designing and implementing effective security strategies. Coupled with insights into risk management, policies, technical controls, and human factors, the book equips readers with the knowledge necessary to navigate the complex cybersecurity landscape. As threats continue to evolve, adhering to these foundational principles remains essential in safeguarding digital assets and maintaining trust in an increasingly digital world.

QuestionAnswer What are the core principles of information security discussed in Whitman's 4th edition? The core principles include confidentiality, integrity, availability, authentication, and non-repudiation, which together form the foundation of effective information security practices. How does Whitman's 4th edition address the evolving landscape of cyber threats? The book emphasizes understanding current threat vectors, risk management strategies, and the importance of adapting security controls to counter emerging cyber threats effectively. What role do policies and procedures play in the principles of information security according to Whitman? Policies and procedures are essential for establishing organizational standards, ensuring consistent security practices, and providing a framework for compliance and incident response. How does Whitman?s 4th edition explain the importance of access control mechanisms? It highlights that access control mechanisms are critical for protecting sensitive information by ensuring only authorized users can access specific resources, thereby maintaining confidentiality and integrity. In what ways does Whitman's book suggest organizations can implement effective security controls based on fundamental principles? The book recommends a layered security approach, incorporating technical controls (like encryption and firewalls), administrative controls (such as policies), and physical controls to uphold the core principles of security.

**Related keywords:** information security, Whitman, principles, 4th edition, cybersecurity, data protection, information assurance, computer security, security policies, risk management

## CRITICAL SECURITY STUDIES AN INTRODUCTION PDF

**Critical Security Studies an Introduction PDF**

Understanding the complexities of security in the modern world requires a comprehensive exploration of critical security studies. The phrase "critical security studies an introduction PDF" often refers to accessible academic resources or downloadable materials that provide foundational insights into this transformative field. This article aims to offer an in-depth overview of critical security studies, its core principles, evolution, and significance, serving as a valuable introduction for students, scholars, and practitioners interested in security analysis from a critical perspective.

## What Are Critical Security Studies?

Critical security studies (CSS) is an interdisciplinary approach that challenges traditional notions of security, emphasizing the importance of analyzing power structures, societal impacts, and broader geopolitical contexts. Unlike conventional security paradigms focused narrowly on state-centric threats such as military invasion or terrorism, CSS questions whose security is prioritized and at what expense.

### Origins and Development

Critical security studies emerged in the late 20th century as a response to the limitations of traditional security paradigms. Influenced by critical theory, post-structuralism, feminism, and other critical approaches, CSS seeks to democratize security analysis and expand its scope.

Key milestones in its development include:

- The influence of the Copenhagen School's securitization theory.
- The rise of post-Cold War security concerns, such as environmental issues, human security, and identity.
- The incorporation of feminist critiques highlighting gendered dimensions of security.

### Core Principles

Critical security studies are grounded in several fundamental principles:

- **Questioning State-Centric Security**: Recognizing that security is not solely about protecting the state but also individuals and communities.
- **Expanding Security Definitions**: Including human security, environmental security, economic security, and social security.
- **Power and Discourse Analysis**: Analyzing how language, narratives, and power relations

shape security agendas.

- **Emphasis on Social Justice**: Highlighting inequalities and advocating for marginalized groups.

## Key Concepts in Critical Security Studies

To grasp CSS fully, understanding its core concepts is essential. These concepts challenge conventional security wisdom and introduce new ways of analyzing threats and responses.

### Securitization Theory

Developed by the Copenhagen School, securitization theory examines how issues are constructed as security threats through speech acts by political actors. It posits that:

- An issue becomes a security threat when authorities declare it so.
- This process enables extraordinary measures and shifts policy priorities.

Implications:

- Not all threats are inherently security threats; it depends on discourse.
- Securitization can be used to justify power grabs or marginalize dissent.

### Human Security

A central theme in CSS, human security broadens the focus from state security to individual well-being. It encompasses:

- Economic security
- Food security
- Health security
- Environmental security
- Personal safety
- Political security

Significance:

- Prioritizes the safety of people over borders.
- Calls for policies that address root causes of insecurity.

### Power, Discourse, and Ideology

CSS emphasizes analyzing how language and narratives influence security policies. It explores:

- How certain issues are framed as threats.
- The role of media, political discourse, and ideology.
- How power relations affect security agendas.

### Critical Perspectives on Security

Various critical approaches contribute unique insights:

- **Feminist Security Studies:** Examines how gender roles influence security dynamics and highlights women's experiences of insecurity.
- **Post-Colonial Security Studies:** Critiques Western-centric security paradigms and emphasizes the impacts of colonialism and imperialism.
- **Environmental Security:** Focuses on ecological threats and climate change as security issues.

## Comparing Traditional and Critical Security Studies

Understanding the distinctions between traditional and critical approaches helps contextualize CSS's revolutionary stance.

### Traditional Security Studies

- Focus on state sovereignty and military threats.
- Emphasize national interests and strategic stability.
- Often rooted in realism and neorealism theories.

### Critical Security Studies

- Broaden security to include human and societal concerns.
- Question the assumptions underpinning state-centric security.
- Advocate for social justice and equality.
- Use interdisciplinary methods and critical theories.

## Importance of Critical Security Studies

CSS offers valuable insights for contemporary security challenges:

- Addresses non-traditional threats like climate change, pandemics, and cyber security.
- Highlights marginalized voices and vulnerable populations.
- Challenges dominant narratives and power structures.
- Promotes more inclusive and equitable security policies.

## Accessing Critical Security Studies PDFs and Resources

For students and researchers interested in exploring critical security studies in depth, numerous PDFs and online resources are available:

### Academic Journals and Articles

- Security Dialogue
- Review of International Studies
- International Political Sociology

These journals often publish open-access articles or PDFs that provide foundational and contemporary insights.

### Key Books and PDFs

- "Critical Security Studies: An Introduction" by Richard Wyn Jones ? often available as PDF online.
- "The Securitization of Climate Change" ? various PDFs exploring environmental security.
- "Gender, Security and the Postcolonial" ? feminist and post-colonial perspectives.

Many of these resources can be found through university libraries, open-access repositories like JSTOR, or academic platforms such as ResearchGate.

### Where to Find Free PDFs

- Google Scholar: Search for specific titles with PDF filters.
- Open Access Journals: Platforms like Directory of Open Access Journals (DOAJ).
- Institutional Repositories: Many universities host free PDFs of theses, dissertations, and course materials.

- ResearchGate and Academia.edu: Researchers often share copies of their papers.

## Conclusion

Critical security studies represent a vital evolution in understanding and analyzing security issues. By challenging traditional paradigms and emphasizing social justice, discourse analysis, and a broader scope of threats, CSS offers a more inclusive and nuanced perspective. Whether accessed through PDFs, books, or academic articles, engaging with critical security studies equips individuals with the analytical tools necessary to navigate and influence the complex security landscape of today and tomorrow.

Understanding these foundational elements and where to find quality PDF resources ensures that learners and scholars can deepen their knowledge and contribute meaningfully to the field. As security concerns continue to evolve beyond conventional threats, critical security studies remain indispensable for fostering more just and resilient societies.

Critical Security Studies An Introduction PDF: A Comprehensive Guide to Understanding the Evolving Landscape of Security

In the rapidly shifting terrain of global politics and international relations, critical security studies an introduction pdf offers scholars, students, and practitioners an invaluable entry point into a transformative approach that challenges traditional notions of security. This field moves beyond classical security paradigms centered solely on military threats and state sovereignty, embracing broader, more nuanced perspectives that consider social, political, economic, environmental, and human dimensions. Whether you're seeking an academic overview or practical insights, understanding the core concepts, debates, and methodologies presented in such an introductory resource is essential for engaging with contemporary security challenges effectively.

Understanding Critical Security Studies: An Overview

Critical security studies emerged as a response to the limitations of traditional security paradigms. Conventional security models?often termed "Realist" or "state-centric"?primarily focus on military threats, territorial integrity, and national sovereignty. While these aspects remain vital, critical security scholars argue that such narrow perspectives overlook many pressing issues that threaten human well-being and global stability.

The Origins and Evolution

- Historical Background: Rooted in the post-World War II order, traditional security studies aimed to address interstate conflicts and military preparedness.

- The Shift in Perspectives: The 1980s and 1990s saw the rise of critical theories, influenced by scholars like the Copenhagen School, post-structuralists, and feminist security studies.
- Main Drivers:
- The end of the Cold War and the recognition of new threats.
- Disillusionment with state-centric models.
- The rise of transnational issues such as climate change, terrorism, and human rights.

Core Principles of Critical Security Studies

Critical security studies challenge the assumptions of traditional security theory, emphasizing the importance of context, power relations, and marginalized voices. The core principles include:

- Security as a Social Construct: Security is not just about military power but also about human well-being and societal stability.
- Broadening the Security Agenda: Addressing issues like economic inequality, environmental degradation, and social injustice.
- De-centering the State: Recognizing that non-state actors and individuals play vital roles in security dynamics.
- Questioning Power Structures: Analyzing how security practices reinforce or challenge existing hierarchies and inequalities.

Key Themes and Topics in Critical Security Studies

- The Concept of Security in a Critical Framework

Traditional security views equate security with the survival of the state. Critical security approaches expand this view by considering:

- Human Security: Focuses on individual safety and dignity?covering health, education, and human rights.
- Environmental Security: Recognizes environmental degradation as a security threat.
- Economic Security: Addresses issues like poverty, inequality, and access to resources.
- Social and Cultural Security: Considers identity, community, and cultural survival.

- Security Discourse and Power Relations

Critical security studies analyze how discourse shapes security policies and perceptions, often

reinforcing power hierarchies. This includes:

- Constructivist Perspectives: How ideas and narratives influence security practices.
- Foucault?s Power/Knowledge: Examining how security is used as a tool of social control.
- The Role of Media and Public Perception: How framing threats influences policy and public opinion.

- Critical Approaches and Methodologies

- Post-Structuralist Methods: Deconstructing dominant security narratives.
- Feminist Security Studies: Highlighting gendered dimensions of security.
- Marxist and Post-Colonial Perspectives: Analyzing how economic and colonial histories shape security.

Major Theoretical Contributions and Thinkers

- The Copenhagen School: Developed the concept of securitization?the process by which issues are framed as security threats to justify extraordinary measures.
- Barry Buzan: Emphasized the importance of sectors?military, political, economic, societal, and environmental.
- Ken Booth: Advocated for human security and questioned the primacy of the state.
- Foucault and Agamben: Offered insights into the relationship between security, power, and sovereignty.

Practical Implications and Policy Relevance

Critical security studies provide frameworks that influence policy-making by:

- Encouraging holistic threat assessments.
- Promoting inclusive security practices that incorporate marginalized groups.
- Challenging militarized approaches in favor of diplomacy, development, and conflict prevention.
- Highlighting the importance of environmental sustainability and social justice in security planning.

Challenges and Criticisms

Despite its valuable insights, critical security studies face several critiques:

- Vagueness and Lack of Policy Prescriptions: Critics argue that broad critiques sometimes lack concrete policy solutions.
- Potential for Relativism: The focus on diverse perspectives may lead to challenges in establishing universal security norms.
- Complexity and Accessibility: Academic language and abstract concepts can be barriers for practitioners and policymakers.

How to Use a PDF Guide on Critical Security Studies

When engaging with a "critical security studies an introduction pdf," consider the following:

- Skim for Structure: Identify key sections such as definitions, theories, case studies, and debates.
- Note Definitions and Key Concepts: Clarify terminology like securitization, human security, and discourse analysis.
- Focus on Case Studies: Real-world examples illustrate how theory applies to current issues.
- Reflect on Critical Perspectives: Think about how these ideas challenge mainstream security policies.
- Use Supplementary Resources: Cross-reference with academic articles, books, and lectures for deeper understanding.

Final Thoughts: Embracing a Broader Security Perspective

The advent of critical security studies an introduction pdf marks an important shift in how we conceptualize threats and responses. It encourages us to question dominant narratives, recognize diverse voices, and adopt more inclusive, sustainable approaches to security. As global challenges become increasingly complex?ranging from climate change to cyber threats?embracing these critical perspectives is essential for developing effective, equitable security policies that safeguard not just territories, but human dignity and planetary health.

In Summary, critical security studies expand the conversation beyond traditional military concerns, urging us to consider social justice, environmental sustainability, and human rights as integral to security. Whether you're an academic, policy maker, or concerned global citizen, engaging deeply with introductory PDFs and foundational texts can equip you with the critical tools needed to navigate and shape the future of security in our interconnected world.

QuestionAnswer What is 'Critical Security Studies: An Introduction' generally about? It provides

an overview of critical security studies, examining how security issues are constructed, the influence of power, and challenging traditional security paradigms to include diverse perspectives. Who are the main authors or contributors of the 'Critical Security Studies: An Introduction' PDF? The book features contributions from scholars such as Richard Wyn Jones, Stéfanie von Hlatky, and others who are prominent in the field of critical security studies. How does critical security studies differ from traditional security studies? Critical security studies challenge the state-centric and militarized focus of traditional security studies, emphasizing human security, social justice, and the role of power relations in shaping security outcomes. What are some key themes covered in the 'Critical Security Studies' PDF? Key themes include the social construction of security, the role of identity and discourse, human security, and the critique of mainstream security policies. Is the 'Critical Security Studies: An Introduction' PDF suitable for beginners? Yes, it is designed to introduce foundational concepts and theories in critical security studies, making it suitable for students and newcomers to the field. Where can I find the 'Critical Security Studies: An Introduction' PDF legally? You can access it through academic libraries, university resources, or purchase it from authorized publishers or platforms that offer legal copies. What is the importance of studying critical security studies through PDFs and online resources? Studying via PDFs and online resources allows for easy access, quick referencing, and the ability to stay updated with the latest debates and scholarly discussions in the field.

**Related keywords:** critical security studies, security studies introduction, security studies PDF, critical security theory, security studies overview, security studies textbook, security studies research, critical security approach, security studies framework, security studies academic

**Read the full article online:** Critical security studies an introduction pdf