Open Source Intelligence Cyberspace La Nuova Frontiera Della Conoscenza

Today, cyber security, cyber defense, information warfare andcyber warfare issues are among the most relevant topics both at thenational and international level. All the major states of the worldare facing cyber threats and trying to understand how cyberspacecould be used to increase power. Through an empirical, conceptual and theoretical approach, CyberConflict has been written by researchers and experts in the fieldsof cyber security, cyber defense and information warfare. It aimsto analyze the processes of information warfare and cyber warfarethrough historical, operational and strategic perspectives of cyberattack. It is original in its delivery because of itsmultidisciplinary approach within an international framework, withstudies dedicated to different states – Canada, Cuba, France,Greece, Italy, Japan, Singapore, Slovenia and South Africa –describing the state's application of information warfareprinciples both in terms of global development and"local" usage and examples. Contents 1. Canada's Cyber Security Policy: a Tortuous Path Towarda Cyber Security Strategy, Hugo Loiseau and Lina Lemay. 2. Cuba: Towards an Active Cyber-defense, Daniel Ventre. 3. French Perspectives on Cyber-conflict, Daniel Ventre. 4. Digital Sparta: Information Operations and Cyber-warfare inGreece, Joseph Fitsanakis. 5. Moving Toward an Italian Cyber Defense and Security Strategy,Stefania Ducci. 6. Cyberspace in Japan's New Defense Strategy, DanielVentre. 7. Singapore's Encounter with Information Warfare: FilteringElectronic Globalization and Military Enhancements, AlanChong. 8. A Slovenian Perspective on Cyber Warfare, Gorazd Praprotnik,Iztok Podbregar, Igor Bernik and Bojan Ticar. 9. A South African Perspective on Information Warfare and CyberWarfare, Brett van Niekerk and Manoj Maharaj. 10. Conclusion, Daniel Ventre

Alternative and Activist New Media provides a rich and accessible overview of the ways in which activists, artists, and citizen groups around the world use new media and information technologies to gain visibility and voice, present alternative or marginal views, share their own DIY information systems and content, and otherwise resist, talk back to, or confront dominant media culture. Today, a lively and contentious cycle of capture, cooptation, and subversion of information, content, and system design marks the relationship between the mainstream 'center' and the interactive, participatory 'edges' of media culture. Five principal forms of alternative and activist new media projects are introduced, including the characteristics that make them different from more conventional media forms and content. The book traces the historical roots of these projects in alternative media, social movements, and activist art, including analyses of key case studies and links to relevant electronic resources. Alternative and Activist New Media will be a useful addition to any course on new media and society, and essential for readers interested in new media activism.

This book is the first one that comprehensively discusses cyberspace sovereignty in China, reflecting China's clear attitude in the global Internet governance: respecting every nation's right to independently choose a development path, cyber management modes and Internet public policies and to participate in the international cyberspace governance on an equal footing. At present, the concept of cyberspace sovereignty is still very strange to many people, so it needs to be thoroughly analyzed. This book will not only help scientific and technical workers in the field of cyberspace security, law researchers and the public understand the development of cyberspace sovereignty at home and abroad, but also serve as reference basis for the relevant decision-making and management departments in their work.

The third edition of The SAGE Handbook of Action Research presents an updated version of the bestselling text, including new chapters covering emerging areas in healthcare, social work, education and international development, as well as an expanded 'skills' section which includes new consultant-relevant materials. Building on the strength of the previous landmark editions, Hilary Bradbury has carefully developed this edition to ensure it follows in their footsteps by mapping the current state of the discipline, as well as looking to the future of the field and exploring the issues at the cutting edge of the action research paradigm today. This volume is an essential resource for scholars and professionals engaged in social and political inquiry, healthcare, international development, new media, organizational research and education.

The new digital media offers us an unprecedented memory capacity,an ubiquitous communication channel and a growing computing power.How can we exploit this medium to augment our personal and socialcognitive processes at the service of human development? Combininga deep knowledge of humanities and social sciences as well as areal familiarity with computer science issues, this bookexplains the collaborative construction of a globalhypercortex coordinated by a computable metalanguage. Byrecognizing fully the symbolic and social nature of humancognition, we could transform our current opaque global brain intoa reflexive collective intelligence.

Intelligent Cities and Globalisation of Innovation Networks combines concepts and theories from the fields of urban development and planning, innovation management, and virtual / intelligent environments. It explains the rise of intelligent cities with respect to the globalisation of systems of innovation; opens up a new way for making intelligent environments via the connection of human skills, institutional mechanisms, and digital spaces operating within a community; and describes a series of platforms and tools for the making of intelligent cities.

Le cyberespace est un objet d'étude très récent pour les sciences sociales. Conflits, crimes et régulations dans le cyberespace contribue au débat scientifique en formation en mettant en avant, par des études de cas, les enjeux internationaux et les questions de méthodes. Cet ouvrage présente le cyberespace comme un système sociotechnique à l'échelle internationale. Il privilégie les acteurs étatiques et non étatiques ainsi que l'étude des normes et des concepts stratégiques. À la différence des études globalisantes, l'approche sociotechnique et l'échelle « méso » permettent d'analyser le cyberespace dans les relations internationales. Il est ici à la fois un espace de collaborations et de conflits pour lequel des modes de régulation spécifiques sont apparus.

Connecting Canadians represents the work of the Community Research Alliance for Community Innovation and Networking (CRACIN), the largest national and international research effort to examine the burgeoning field of community informatics, a cross-disciplinary approach to the mobilization of information and communications technologies (ICT) for community change. Funded for four years by the SSHRC's Initiative for the New Economy, CRACIN systematically studied a wide variety of Canadian community ICT initiatives, bringing perspectives from sociology, computer science, critical theory, women's studies, library and information sciences, and management studies to bear on networking technologies. A comprehensive thematic account of this in-depth research, Connecting Canadians will be an essential resource for NGOs, governments, the private sector, and multilateral agencies across the globe.

Open innovation increases the profit of companies and organizations via the input and the adoption of new ideas that are transformed into new processes, products, and services. Yet, how do we ensure that adopters of such innovations focus on relevant problems and use appropriate methods? How should we manage open innovation technologies? How can we exploit distributed knowledge and inventions? And how can we promote them successfully on the market? With valuable lessons to be learned from academic research and industrial experiences of e.g. Intel, Nokia, Philips Healthcare, small municipalities, e-learning platforms and user communities, this book focuses on some of the key dimensions of open innovation and open innovation technologies. It is divided into three themes: theme 1 deals with open innovation as it is in use today, including theoretical underpinnings and lessons from related research fields. Theme 2 analyzes the use of open innovation in organizations today in order to extract best practices. Theme 3 presents forward-looking theoretical research as well as practical future uses of open innovation. Each chapter addresses the particular topics by presenting experiences and results gained in real life projects and/or by empirical research, and clearly states its purpose and how readers are supposed to benefit from it. Overall, the objectives of this book are to advance and disseminate research on systematic open innovation, and to make its results available to practitioners. Thus, the intended target audience includes the international academic community, industrial enterprises, and public authorities.

Open source, intelligence & cyberspace. La nuova frontiera della conoscenzaLa Cina e la Nuova Via della SetaProgetto per un'invasione globaleRubbettino EditoreCyber Espionage e Cyber CounterintelligenceSpionaggio e controspionaggio ciberneticoRubbettino EditoreCyberspace SovereigntyReflections on building a community of common future in cyberspaceSpringer

Les bibliothèques numériques qui émergent des « sociétés de l'information » ne concernent plus uniquement ces dispositifs numériques technodocumentaires patrimonialement, culturellement ou scientifiquement déterminés. Les réseaux sociaux et les sites marchands à forte audience partagent les mêmes technologies, proposent des fonctionnalités d'expérience utilisateur (UX) identiques, des ressources numériques hétérogènes et naissent au sein des mêmes communautés de concepteurs et d'ingénieurs. Bibliothèque numérique et innovation montre ces recouvrements induits par la technologie, qui nourrissent un imaginaire de l'usage. Ce dernier irrigue un mouvement de transformation de l'innovation où usage et usager/utilisateur occupent une place centrale. Cette deuxième édition révisée et augmentée interroge le phénomène des données ouvertes liées et observe leurs impacts sur l'évolution des bibliothèques numériques. Des agencements inédits portés par les interopérabilités technologiques font émerger des biens informationnels communs que de nouvelles communautés épistémiques peuvent créer, ré-agencer et enrichir dans une compréhension citoyenne de la société de l'information.

This book investigates the intersection of terrorism, digital technologies and cyberspace. The evolving field of cyber-terrorism research is dominated by single-perspective, technological, political, or sociological texts. In contrast, Terrorism Online uses a multi-disciplinary framework to provide a broader introduction to debates and developments that have largely been conducted in isolation. Drawing together key academics from a range of disciplinary fields, including Computer Science, Engineering, Social Psychology, International Relations, Law and Politics, the volume focuses on three broad themes: 1) how – and why – do terrorists engage with the Internet, digital technologies and cyberspace?; 2) what threat do these various activities pose, and to whom?; 3) how might these activities be prevented, deterred or addressed? Exploring these themes, the book engages with a range of contemporary case studies and different forms of terrorism: from lone-actor terrorists and protest activities associated with 'hacktivist' groups to state-based terrorism. Through the book's engagement with questions of law, politics, technology and beyond, the volume offers a holistic approach to cyberterrorism which provides a unique and invaluable contribution to this subject matter. This book will be of great interest to students of cybersecurity, security studies, terrorism and International Relations.

This book offers a philosophical exploration of lines in art and culture, and traces their history from Antiquity onwards. Lines can be physical phenomena, cognitive responses to observed processes, or both at the same time. Based on this assumption, the book describes the "philosophy of lines" in art, architecture, and science. The book compares Western and Eastern traditions. It examines lines in the works of Paul Klee, Wassily Kandinsky, and Henri Michaux, as well as in Chinese and Japanese art and calligraphy. Lines are not merely a matter of aesthetics but also reflect the psychological states of entire cultures. In the nineteenth century, non-Euclidean geometry sparked the phenomenon of the "self-negating line," which influenced modern art; it also prepared the ground for virtual reality. Straight lines, distorted lines, blurred lines, hot and cold lines, dynamic lines, lines of force, virtual lines, and on and on, lines narrate the development of human civilization. Thorsten Botz-Bornstein is Associate Professor of philosophy at Gulf University for Science and Technology in Kuwait.

This volume shows us that in order to deal with today's Fourth Generation asymmetric warfare by terrorist groups using conventional arms and weapons of mass destruction, we need a new 'global networked' approach. The contributors examine the various attempts that have been made to counter the latest wave of terrorism, including the US strikes against Afghanistan and Iraq, President George W. Bush's declaration of a 'war against terrorism', the creation of the US Department of Homeland Security, and the 9/11 Commission. Drawing from our experience with 'Terrorism Early Warning' and the co-production of counter-terrorism intelligence, this book explains the need for such a network and shows how it could be formed. It compiles the opinions of experts from clinical medicine, public policy, law enforcement and the military. These expert contributors identify the nature of a global counter-terrorism network, show how it could be created, and provide clear guidelines for gauging its future effectiveness. This book will be of great interest to all students of terrorism studies, US national security, international relations, and political science in general.

Fourth Edition (Traditional Chinese Translation) Sheds New Light on Open Source Intelligence Collection and Analysis. Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in

great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Owner Information Twitter GPS & Account Data Hidden Photo GPS & Metadata Deleted Websites & Posts Website Owner Information Alias Social Network Profiles Additional User Accounts Sensitive Documents & Photos Live Streaming Social Content IP Addresses of Users Newspaper Archives & Scans Social Content by Location Private Email Addresses Hidden Personal Videos Duplicate Copies of Photos Personal Radio Communications Compromised Email Information Wireless Routers by Location Hidden Mapping Applications Complete Facebook Data Free Investigative Software Alternative Search Engines Mobile App Network Data Unlisted Addresses Unlisted Phone Numbers Useful Browser Extensions Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity

Explorations of the new frontiers of cybertext and cyberspace culture.

This book explores a range of biohealth and biosecurity threats, places them in context, and offers responses and solutions from global and local, networked and pyramidal, as well as specialized and interdisciplinary perspectives.

O livro é destinado aos operadores do Direito, especialistas em Direito Digital, sociólogos e antropólogos preocupados com a sociedade da informação e profissionais de tecnologia. O livro aborda, entre outros assuntos, a dimensão jurídica do governo eletrônico no Brasil, a informatização do processo judicial, assim como a infra-estrutura de chaves públicas no Brasil e a interoperabilidade como um princípio do e-gov e sua relação com os padrões tecnológicos abertos.

In the past year, Information Operations (IO) has matured from an early emphasis on the protection of critical infrastructures and against electronic espionage and is now more focused on content and on interagency information-sharing. The value of information--all information, not only secret information--and the value of global monitoring in all languages, 24/7, has been clearly established by the Undersecretary of Defense for Intelligence (USDI). This monograph defines and discusses three IO elements: Strategic Communication (the message); Open Source Intelligence (the reality); and, Joint Information Operations Centers (the technology). It concludes with a strategic overview of the various conceptual and technical elements required to meet modern IO needs, and provides a requirements statement that could be tailored to the needs of any Combatant Commander, service, or agency.

This SpringerBrief gives the reader a detailed account of how cybersecurity in Israel has evolved over the past two decades. The formation of the regions cybersecurity strategy is explored and an in-depth analysis of key developments in cybersecurity policy is provided. The authors examine cybersecurity from an integrative national perspective and see it as a set of policies and actions with two interconnected goals: to mitigate security risks and increase resilience and leverage opportunities enabled by cyber-space. Chapters include an insight into the planning and implementation of the National Security Concept strategy which facilitated the Critical Infrastructure Protection (CIP) agreement in 2002, (one of the first of its kind), the foundation of the Israeli Cyber-strategy in 2011, and details of the current steps being taken to establish a National Cyber Security Authority (NCSA). Cybersecurity in Israel will be essential reading for anybody interested in cyber-security policy, including students, researchers, analysts and policy makers alike.

This new book brings together leading terrorism scholars and defence professionals to discuss the impact of networks on conflict and war. Post-modern terrorism and topics of global insurgency are also comprehensively covered. The text is divided into four sections to cover the key areas: introductory/overview, theory, terrorism and global insurgency, Al Qaeda focus, and networks. Eminent contributors include John Arquilla and David Ronfeldt, Brian Jenkins, Stephen Sloan, Graham Turbiville, and Max Manwaring. This book was previously published as a special issue of the leading journal Low Intensity Conflict and Law Enforcement.

This report examines Russia's military and diplomatic campaign in Syria, the largest and most significant Russian out-of-area operation since the end of the Cold War. Russia's experience in Syria will shape its military thinking, influence promotion and personnel decisions, impact research and development for its arms industry, and expand its influence in the Middle East and beyond for the foreseeable future. Yet despite the importance of Russia's involvement in Syria—especially as the United States competes with countries such as Russia and China—there has been little systematic analysis of Russia's campaign in Syria. This research aims to help fill the gap and provides some new analysis and data. It conducts a broad assessment of the Russian campaign—including political objectives, diplomatic initiatives, and civilian targeting—which places the military campaign in a wider context. In addition, it compiles a data set of Russia's civilian targeting and analyzes satellite imagery of Russian activity. Overall, this report concludes that Russia was relatively successful in achieving its main near-term political and military objectives in Syria, including preventing the collapse of the Assad regime (an important regional partner) and thwarting a possible U.S. attempt to overthrow Assad. Still, Russia used a systematic punishment campaign that involved attacks against civilian and humanitarian infrastructure in an attempt to deny resources—including food, fuel, and medical aid—to the opposition while simultaneously eroding the will of civilians to support opposition groups.

Conferences Proceedings of 20th European Conference on Cyber Warfare and Security

This book considers key ethical questions in museum policy and practice, particularly those related to issues of collection and display. What does a collection signify in the twenty-first century

museum? How does an engagement with immateriality challenge museums' concept of ownership, and how does that immateriality translate into the design of exhibitions and museum space? Are museums still about safeguarding objects, and what does safeguarding mean for diverse individuals and communities today? How does the notion of the museum as a performative space challenge our perceptions of the object? The scholarship represented in this volume is a testament to the range and significance of critical inquiry in museum ethics. Together, the chapters resist a legalistic interpretation, bound by codes and common practice, to advance an ethics discourse that is richly theorized, constantly changing and contingent on diverse external factors. Contributors take stock of innovative research to articulate a new museum ethics founded on the moral agency of museums, the concept that museums have both the capacity and the responsibility to create social change. This book is based on a special issue of Museum Management and Curatorship.

The central purpose of this collection of essays is to make a creative addition to the debates surrounding the cultural heritage domain. In the 21st century the world faces epochal changes which affect every part of society, including the arenas in which cultural heritage is made, held, collected, curated, exhibited, or simply exists. The book is about these changes; about the decentring of culture and cultural heritage away from institutional structures towards the individual; about the questions which the advent of digital technologies is demanding that we ask and answer in relation to how we understand, collect and make available Europe's cultural heritage. Cultural heritage has enormous potential in terms of its contribution to improving the quality of life for people, understanding the past, assisting territorial cohesion, driving economic growth, opening up employment opportunities and supporting wider developments such as improvements in education and in artistic careers. Given that spectrum of possible benefits to society, the range of studies that follow here are intended to be a resource and stimulus to help inform not just professionals in the sector but all those with an interest in cultural heritage.

As an increasing amount of information is made available online, the assumption is that people who visit Web sites will be able to strategize their learning to optimize access to this information. Constructing Self-Discovery Learning Spaces Online: Scaffolding and Decision Making Technologies raises awareness of the strategies supporting self-driven learner efficacy on a number of site types. This book reflects on existing literature about self-discovery learning and what learners need in terms of scaffolding to help them make the right decisions, assess their own level of learning, vet information strategically, collaborate with other learners, and build their own skill sets.

This book brings together and reviews different disciplinary approaches to digital information and communication systems across the social sciences. It synthesises the developments of the Internet Age, and the micro and macro consequences of these developments.

"This book offers a look at the latest research within digital literacy and competence, setting the bar for the digital citizen of today and tomorrow"--Provided by publisher.

This book reports on the latest research and developments in the field of cybersecurity, placing special emphasis on personal security and new methods for reducing human error and increasing cyber awareness, as well as innovative solutions for increasing the security of advanced Information Technology (IT) infrastructures. It covers a broad range of topics, including methods for human training; novel Cyber-Physical and Process-Control Systems; social, economic, and behavioral aspects of cyberspace; issues concerning the cybersecurity index; security metrics for enterprises; risk evaluation, and many others. Based on the AHFE 2017 International Conference on Human Factors in Cybersecurity, held on July 17–21, 2017, in Los Angeles, California, USA, the book not only presents innovative cybersecurity technologies, but also discusses emerging threats, current gaps in the available systems, and future challenges that may be successfully overcome with the help of human factors research.

Digital Labor calls on the reader to examine the shifting sites of labor markets to the Internet through the lens of their political, technological, and historical making. Internet users currently create most of the content that makes up the web: they search, link, tweet, and post updates—leaving their "deep" data exposed. Meanwhile, governments listen in, and big corporations track, analyze, and predict users' interests and habits. This unique collection of essays provides a wide-ranging account of the dark side of the Internet. It claims that the divide between leisure time and work has vanished so that every aspect of life drives the digital economy. The book reveals the anatomy of playbor (play/labor), the lure of exploitation and the potential for empowerment. Ultimately, the 14 thought-provoking chapters in this volume ask how users can politicize their troubled complicity, create public alternatives to the centralized social web, and thrive online. Contributors: Mark Andrejevic, Ayhan Aytes, Michel Bauwens, Jonathan Beller, Patricia Ticineto Clough, Sean Cubitt, Jodi Dean, Abigail De Kosnik, Julian Dibbell, Christian Fuchs, Lisa Nakamura, Andrew Ross, Ned Rossiter, Trebor Scholz, Tizania Terranova, McKenzie Wark, and Soenke Zehle

Reconciling Copyright with Cumulative Creativity: The Third Paradigm examines the long history of creativity, from cave art to digital remix, in order to demonstrate a consistent disparity between the traditional cumulative mechanics of creativity and modern copyright policies. Giancarlo Frosio calls for the return of creativity to an inclusive process, so that the first (pre-modern imitative and collaborative model) and second (post-Romantic copyright model) creative paradigms can be reconciled into an emerging third paradigm which would be seen as a networked peer and user-based collaborative model.

Now almost 20 years old, the digital turn in architecture has already gone through several stages and phases. Architectural Design (AD) has captured them all – from folding to cyberspace, nonlinearity and hypersurfaces, from versioning to scripting, emergence, information modelling and parametricism. It has recorded and interpreted the spirit of the times with vivid documentary precision, fostering and often anticipating crucial architectural and theoretical developments. This anthology of AD's most salient articles is chronologically and thematically arranged to provide a complete historical timeline of the recent rise to pre-eminence of computer-based design and production. Mario Carpo provides an astute overview of the recent history of digital design in his comprehensive introductory essay and in his leaders to each original text. A much needed pedagogical and research tool for students and scholars, this synopsis also relates the present state of digitality in architecture to the history and theory of its recent development and trends, and raises issues of crucial importance for the contemporary practice of the design professions. A comprehensive anthology on digital architecture edited by one of its most eminent scholars in this field, Mario Carpo. Includes seminal texts by Bernard Cache, Peter Eisenman, John Frazer, Charles Jencks, Greg Lynn, Achim Menges and Patrik Schumacher. Features key works by FOA, Frank Gehry, Zaha Hadid, Ali Rahim, Lars Spuybroek/NOX, Kas Oosterhuis and SHoP.

This book presents 12 essays that focus on the analysis of the problems prompted by cyber operations (COs). It clarifies and discusses the ethical and regulatory problems raised by the deployment of cyber capabilities by a state's army to inflict disruption or damage to an adversary's targets in or through cyberspace. Written by world-leading philosophers, ethicists, policy-makers, and law and military experts, the essays cover such topics as the conceptual novelty of COs and the ethical problems that this engenders; the applicability of existing conceptual and regulatory frameworks to COs deployed in case of conflicts; the definition of deterrence strategies involving COs; and the analysis of models to foster cooperation in managing cyber crises. Each essay is an invited contribution or a revised version of a paper originally presented at the workshop on Ethics and Policies for Cyber Warfare, organized by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Oxford. The

volume endorses a multi-disciplinary approach, as such it offers a comprehensive overview of the ethical, legal, and policy problems posed by COs and of the different approaches and methods that can be used to solve them. It will appeal to a wide readership, including ethicists, philosophers, military experts, strategy planners, and law- and policy-makers.

The primary function of the intelligence analyst is to make sense of information about the world, but the way analysts do that work will look profoundly different a decade from now. Technological changes will bring both new advances in conducting analysis and new risks related to technologically based activities and communications around the world. Because these changes are virtually inevitable, the Intelligence Community will need to make sustained collaboration with researchers in the social and behavioral sciences (SBS) a key priority if it is to adapt to these changes in the most productive ways. A Decadal Survey Of The Social and Behavioral Sciences provides guidance for a 10-year research agenda. This report identifies key opportunities in SBS research for strengthening intelligence analysis and offers ideas for integrating the knowledge and perspectives of researchers from these fields into the planning and design of efforts to support intelligence analysis.

Recommended online resources p. 476.481