This Machine Kills Secrets How Wikileakers Cypherpunks And Hacktivists Aim To The Worlds Information Andy Greenberg

???????????·???????"??? ?????????"?? ??"????"?"????"??????????? ?????????????????·??? ???????????????????????????

??????????? ????????????14000???????? ?????????Top.1?????????100?? ?????20????? ???????CBS Films????????? ??????????????????? ??????????? ??????????? ??? ???????????????????????????……

???——???????? ??…… ???????????????????? ????????????????????1918??? ??

???…… ??????????????????????? ???????????????????????? ??????????? ??????????? ???????????????? ????????PanSci???????? ????????? ???????????????? ????????????????????????? ?????PanSci???????? ???????????

?? ——???????? ?? ??24??????????????????????????????? ?????????????????????????????? ——????????????????

??? ——???????PanSci?????????

?? ——??? ?????????????????? ??????????????????????????????????——????????????????????????????????? ——?? ?? ——????? ?? ——??? ????????????? ?? ????? ——Ashley ???????????? ???????????????????? ——Holly Y ??????????????????????????? ——Katya Taylor ??????????????????????????????? ——Amazonian ??? ????(??)

????????????OPC???? ??????Amazon???? Amazon.com???????????????????????? ?????? ??Axios??????Business Insider???????TechCrunch???????Fast Company?????????????Anne Applebaum????????????Steven Levy? ?????????????????????? ??????????? 2014?????????? ?????????????????????????????????2017??????????????NotPetya???????????????????????? ?? ?????????????????Sandworm?? ????????????? ?????????Andy Greenberg????????Wired??????????????????????????????? ??????????????????????????????????Gerald Loeb Award for International Reporting?? ???? ??? ???????????????????????????????????????

In 2013, Edward Snowden released a trove of documents revealing the extent of government electronic surveillance. Since then, we have been inundated with reports of vicious malware attacks, election hacking, data breaches, potential cyberwars, fights over Net Neutrality, and

fake internet news. Where once discussion of cyberspace was full of hope of incredible potential benefits for humanity and global connection, it has become the domain of fear, anxiety, conflict, and authoritarian impulses. As the cloud of the Net darkens into a storm, are there insights from Christian theology about our online existence? Is the divine present in this phenomenon known as cyberspace? Is it a realm of fear or a realm of hope? In The Cyberdimension, Eric Trozzo engages these questions, seeking not only a theological means of speaking about cyberspace in its ambiguity, but also how the spiritual dimension of life provokes resistance to the reduction of life to what can be calculated. Rather than focusing on the content available online, he looks to the structure of cyberspace itself to find a chastened yet still expectant vision of divinity amidst the political, economic, and social forces at play in the cyber realm.

From the rise of cyberbullying and hactivism to the issues surrounding digital privacy rights and freedom of speech, the Internet is changing the ways in which we govern and are governed as citizens. This book examines how citizens encounter and perform new sorts of rights, duties, opportunities and challenges through the Internet. By disrupting prevailing understandings of citizenship and cyberspace, the authors highlight the dynamic relationship between these two concepts. Rather than assuming that these are static or established "facts" of politics and society, the book shows how the challenges and opportunities presented by the Internet inevitably impact upon the action and understanding of political agency. In doing so, it investigates how we conduct ourselves in cyberspace through digital acts. This book provides a new theoretical understanding of what it means to be a citizen today for students and scholars across the social sciences. This new and updated edition includes two new chapters. A Preface consists of reflections on developments in digital politics since the book was published in 2015. It considers how recent major political struggles over digital technologies and data can be understood in relation to the conceptualization of digital citizens that the book offers. While the Preface positions dominant responses to these struggles such as government regulations as 'closings', a new final chapter, Digital citizens-yet-to-come offers examples of 'openings' – digital acts such as new forms of data activism that are less recognised but which point to the emergence of paradoxical digital acts that are producing new digital political subjectivities.

Traditional Chinese edition of Paper Towns by John Green, a science fiction thriller. In Traditional Chinese. Distributed by Tsai Fong Books, Inc.

????????????????????? ???????????????????????????????? ?? ??????????? ?? ????????????? ?? ???????????????????????????????? ?? ?? ????????????????????????? ??Google??????Apple??? ?? ???????????????????????????????????????DARPA??? ???????????????????? - James Ledbetter, Inc. ???? ???? ??????? ????????Scott Malcomson??????????????????????????????????New York Times????????New Yorker???2004?2011???????????New York Times Magazine?? ???????Tuturani?????????????1 990?????????????????????????1994???????????????2000???????????????????????2000?????????????????????????????????9/11???????????????????2010????????????????????????? ???? ??? ?? ???6????????…...?????????????????? ?????????????????

Lifelong learning can occur both in and out of the classroom, but the most valuable instruction takes place on the job. Remote Workforce Training: Effective Technologies and Strategies investigates methods, techniques, and systems used in employee training programs. The tools and technologies surveyed within these pages will help employers take their workers beyond the transient skill sets offered by university degrees and into a constant state of learning and practice that will enhance both their productivity and technical abilities on a regular basis. In particular, the knowledge offered by this reference book will be of use to educators and students as well as managers, leaders, administrators, and personnel.

Originally published in hardcover in 2019 by Doubleday.

This book provides an in-depth exploration of the phenomenon of hacking from a multidisciplinary perspective that addresses the social and technological aspects of this unique activity as well as its impact. • Documents how computer hacking fits into various forms of cybercrime • Describes the subculture of computer hackers and explains how this social world plays an integral role in the business of hacking • Clarifies the subtle differences between ethical and malicious hacks • Focuses on the non-technical aspects of computer hacking to enable the reader to better understand the actors and their motives

This work explores the relationships between legal institutions and political and economic transformation. It argues that as law is enlisted to help produce the profound economic and sociotechnical shifts that have accompanied the emergence of the informational economy, it is changing in fundamental ways.

The fascinating untold story of digital cash and its creators—from experiments in the 1970s to the mania over Bitcoin and other cryptocurrencies Bitcoin may appear to be a revolutionary form of digital cash without precedent or prehistory. In fact, it is only the best-known recent experiment in a long line of similar efforts going back to the 1970s. But the story behind cryptocurrencies like Bitcoin and its blockchain technology has largely been untold—until now. In Digital Cash, Finn Brunton reveals how technological utopians and political radicals created experimental money to bring about their visions of the future: to protect privacy, bring down governments, prepare for apocalypse, or launch a civilization of innovation and abundance that would make its creators immortal. Filled with marvelous characters, stories, and ideas, Digital Cash is an engaging and accessible account of the strange origins and remarkable technologies behind today's cryptocurrency explosion.

The militarized legacy of the digital cloud: how the cloud grew out of older network technologies and politics.

This second edition of Hong Kong Media Law is an authoritative guide to the laws most important to reporters, editors, news executives and other professionals working for the print, online and broadcast media—and the lawyers who advise them. Topics include defamation, court reporting, privacy, access to information, copyright, newsgathering and reporting restrictions. The book also examines

legal hurdles Hong Kong and international journalists face while reporting on the mainland of the People's Republic of China. Also featured are chapter FAQs and checklists, a glossary of legal terms, a research guide and key legislation texts. Hackers as vital disruptors, inspiring a new wave of activism in which ordinary citizens take back democracy. Hackers have a bad reputation, as shady deployers of bots and destroyers of infrastructure. In Coding Democracy, Maureen Webb offers another view. Hackers, she argues, can be vital disruptors. Hacking is becoming a practice, an ethos, and a metaphor for a new wave of activism in which ordinary citizens are inventing new forms of distributed, decentralized democracy for a digital era. Confronted with concentrations of power, mass surveillance, and authoritarianism enabled by new technology, the hacking movement is trying to "build out" democracy into cyberspace.
Traditional Chinese Edition of [Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers]
Who Are The Cypherpunks? This is the unauthorized telling of the revolutionary cryptography story behind the motion picture The Fifth Estate in theatres this October, and We Steal Secrets: The Story of Wikileaks, a documentary out now. WikiLeaks brought to light a new form of whistleblowing, using powerful cryptographic code to hide leakers' identities while they spill the private data of government agencies and corporations. But that technology has been evolving for decades in the hands of hackers and radical activists, from the libertarian enclaves of Northern California to Berlin to the Balkans. And the secret-killing machine continues to evolve beyond WikiLeaks, as a movement of hacktivists aims to obliterate the world's institutional secrecy. Forbes journalist Andy Greenberg has traced its shadowy history from the cryptography revolution of the 1970s to Wikileaks founding hacker Julian Assange, Anonymous, and beyond. This is the story of the code and the characters—idealists, anarchists, extremists—who are transforming the next generation's notion of what activism can be. With unrivaled access to such major players as Julian Assange, Daniel Domscheit-Berg, and WikiLeaks' shadowy engineer known as the Architect, never before interviewed, Greenberg unveils the world of politically-motivated hackers—who they are and how they operate.
This book encourages cybersecurity professionals to take a wider view of what cybersecurity means, and to exploit international standards and best practice to create a culture of cybersecurity awareness within their organization that supplements technology-based defenses.
??????·?????????????.???????????????????.?????????——???????????????????? ????????????????????.?????????????——??????????????.
This Machine Kills SecretsJulian Assange, the Cypherpunks, and Their Fight to Empower WhistleblowersPenguin
The rapid evolution of technology continuously changes the way people interact, work, and learn. By examining these advances from a sociological perspective, researchers can further understand the impact of cyberspace on human

behavior, interaction, and cognition. Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications is a vital reference source covering the impact of social networking platforms on a variety of relationships, including those between individuals, governments, citizens, businesses, and consumers. The publication also highlights the negative behavioral, physical, and mental effects of increased online usage and screen time such as mental health issues, internet addiction, and body image. Showcasing a range of topics including online dating, smartphone dependency, and cyberbullying, this multi-volume book is ideally designed for sociologists, psychologists, computer scientists, engineers, communication specialists, academicians, researchers, and graduate-level students seeking current research on media usage and its behavioral effects.

Commentators have shown how a 'culture of security' ushered in after the terrorist attacks of 11 September 2001 has involved exceptional legal measures and increased recourse to secrecy on the basis of protecting public safety and safeguarding national security. In this context, scholars have largely been preoccupied with the ways that increased security impinges upon civil liberties. While secrecy is justified on public interest grounds, there remains a tension between the need for secrecy and calls for openness, transparency and disclosure. In law, secrecy has implications for the separation of powers, due process, and the rule of law, raising fundamental concerns about open justice, procedural fairness and human rights. Beyond the counterterrorism and legal context, scholarly interest in secrecy has been concerned with the credibility of public and private institutions, as well as the legacies of secrecy across a range of institutional and cultural settings. By exploring the intersections between secrecy, law and society, this volume is a timely and critical intervention in secrecy debates traversing various fields of legal and social inquiry. It will be a useful resource for academic researchers, university teachers and students, as well as law practitioners and policymakers interested in the legal and socio-legal dimensions of secrecy.

This volume addresses the major questions surrounding a concept that has become ubiquitous in the media and in civil society as well as in political and economic discourses in recent years, and which is demanded with increasing frequency: transparency. How can society deal with increasing and often diverging demands and expectations of transparency? What role can different political and civil society actors play in processes of producing, or preventing, transparency? Where are the limits of transparency and how are these boundaries negotiated? What is the relationship of transparency to processes of social change, as well as systems of social surveillance and control? Engaging with transparency as an interrelated product of law, politics, economics and culture, this interdisciplinary volume explores the ambiguities and contradictions, as well as the social and political dilemmas, that the age of transparency has unleashed. As such it will appeal to researchers across the social sciences and

humanities with interests in politics, history, sociology, civil society, citizenship, public policy, criminology and law.

???????????????? ,etc.????all in?? ???????????????????????? ???????????????????????????????????? ??????????? ??????????????????????? ????????????Bloomberg Markets???????? ?????????????????? ??????????????????????????????????? ??????????????????????????????? ?????????????????????????????????? ???????——

?????????2.6??????????????????? Paypal ???????????Visa?????USDC ????????????? Microstrategy?????Square ??????????????????? NFT???????????????????? ??????????????????????????? SpaceX????????????????????????……?? ??????????????????????? ?????2009???????????????????? ???????????????????????????????????? ?? ????????????????????????????????? ?? ??????????? ?? ??? ?? ?????????????????? ?????????????????????? ?????????????????????????????? ????? ???????Finn Brunton? ??? ??? ???????????Spam: A Shadow History of the Internet????????????Communication and Obfuscation: A User's Guide for Privacy and Protest????????????????????????????????? ????? ??? ????????????? ??? ???????·???????·????????????????????????????????,????????????????

Many of today's organizations "live in public"; they devote extensive resources to branding, catching the public eye, and capitalizing on the age of transparency. But, at the same time, a growing number of companies and other collectives are flying under the radar, concealing their identities and activities. This book offers a framework for thinking about how organizations and their members communicate identity to relevant audiences. Considering the degree to which organizations reveal themselves, the extent to which members express their identification with the organization, and whether the audience is public or local, author Craig R. Scott describes collectives as residing in "regions" that range from transparent to shaded, from shadowed to dark. Taking a closer look at groups like EarthFirst!, the Church of Scientology, Alcoholics Anonymous, the KKK, Skull and Bones, U.S. special mission units, men's bathhouses, and various terrorist organizations, this book draws attention to shaded, shadowed, and dark collectives as important organizations in the contemporary landscape.

???????????????????????? ??????????????????? ????????????????? ????????????? ????????? ??????????????????????????????????? ? ??????????????????????????????????? ?

?? ? ??????????????????????????? ? ???????????????????????? ? ??13?????????????????????????????? ? ??? ?????????? ??????????????? 2014? ??? ???? 3??? ??? ???????????????????…… ???????????? ??????????????????????? ??????????????????? ????????????????????????????????????? ?????????????????????? ??????24?????????????????????????????? ????????????????? ?????????????????3.9?????????????4.9?? ????????5????????????????? ?1?????OCEAN???????????????????????????? ?2?????????????????????????????? ?3?????????????????????????? ?4???????app????????????????????????? ?5???????????????24????????????????????? ?Facebook???????????????? ?????????? ????????????…… ????????Facebook???????? ?????????18????????5,000??????????2.4?????? ????????Google???????? ????????????????????????????????????? ?????????????????20????? ??????????????????? ????????????…… ??????????????????????????????? ??????????????????????? ?????????????????????? ???????????????? ?? ??????????? ???????Facebook?Google?Twitter? ?????????????????…… Facebook?Twitter?????????????? ??????????????????????????? ?????????????????????????? Google????????????????? ?????????????????????????? ????????????????????30?????????????Facebook? ??????????????? ???????????????????????????????????? ?????????????????????????????????? ?????????????????????? ?????4??????????? ??????????????????????????????

A guide to journalistic ethics for today's digital technologies With contributions from an international panel of experts on the topic, News Media Innovation Reconsidered offers a guide for the revitalizing of the ethical and civil ideals of journalism. The authors discuss how to energize journalistic practices and products and explore how to harness the power of digital technological innovations such as immersive journalism, the automatization and personalization of news, newsgames, and artificial-intelligence news production. The book presents an innovative framework of "creative reconstruction" and reviews new journalistic concepts, models, initiatives, and practices that clearly demonstrate professional ethics that embrace truth seeking, transparency, fact checking, and accuracy, and other ethical considerations. While the contributors represent numerous countries, many of examples are drawn from the Spanish-speaking media and can serve as models for an international audience. This important book: Explores the impact on the news media from mobile-first, virtual reality, and artificial intelligence-driven platforms Examines the challenges of

maintaining journalistic ethics in today's digital world Demonstrates how to use technology to expose readers to news outside their comfort zones Provides information for discerning truth from fake news Written for researchers, students in journalism and communication programs, New Media Innovation Reconsidered offers a much-needed guide for recreating journalistic ethics in our digital age.

Combining cutting edge theories with empirical research, this timely book offers an in-depth analysis of current platform-based radical movements to show how digital technologies revolutionise political and economic organising. This is an invaluable contribution to the emerging literature on the relationship between technology and society.

With its conceptual innovations and case studies, Whistleblowers clarifies the much-discussed but under-studied phenomena of leaking and whistleblowing, with a particular focus on the collaborative networks that make the extraction and publication of secrets possible.

How we can evade, protest, and sabotage today's pervasive digital surveillance by deploying more data, not less—and why we should. With Obfuscation, Finn Brunton and Helen Nissenbaum mean to start a revolution. They are calling us not to the barricades but to our computers, offering us ways to fight today's pervasive digital surveillance—the collection of our data by governments, corporations, advertisers, and hackers. To the toolkit of privacy protecting techniques and projects, they propose adding obfuscation: the deliberate use of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects. Brunton and Nissenbaum provide tools and a rationale for evasion, noncompliance, refusal, even sabotage—especially for average users, those of us not in a position to opt out or exert control over data about ourselves. Obfuscation will teach users to push back, software developers to keep their user data safe, and policy makers to gather data without misusing it. Brunton and Nissenbaum present a guide to the forms and formats that obfuscation has taken and explain how to craft its implementation to suit the goal and the adversary. They describe a series of historical and contemporary examples, including radar chaff deployed by World War II pilots, Twitter bots that hobbled the social media strategy of popular protest movements, and software that can camouflage users' search queries and stymie online advertising. They go on to consider obfuscation in more general terms, discussing why obfuscation is necessary, whether it is justified, how it works, and how it can be integrated with other privacy practices and technologies.

We live in an age of surveillance. In this book, the moral importance of this is explained through an examination of virtual identities.

??

Experts from MIT explore recent advances in cybersecurity, bringing together management, technical, and sociological perspectives. Ongoing cyberattacks, hacks, data breaches, and privacy concerns demonstrate vividly the inadequacy of existing methods of cybersecurity and the need to develop new and better ones. This book brings together experts from across MIT to explore recent advances in cybersecurity from management, technical, and sociological perspectives. Leading researchers from MIT's Computer Science & Artificial Intelligence Lab, the MIT Media Lab, MIT Sloan School of Management, and MIT Lincoln Lab, along with their counterparts at Draper Lab, the University of Cambridge, and SRI, discuss such varied topics as a systems perspective on managing risk, the development of inherently secure hardware, and the Dark Web. The contributors suggest approaches that range from the market-driven to the theoretical, describe problems that arise in a decentralized, IoT world, and reimagine what optimal systems architecture and effective management might look like. Contributors YNadav

Aharon, Yaniv Altshuler, Manuel Cebrian, Nazli Choucri, André DeHon, Ryan Ellis, Yuval Elovici, Harry Halpin, Thomas Hardjono, James Houghton, Keman Huang, Mohammad S. Jalali, Priscilla Koepke, Yang Lee, Stuart Madnick, Simon W. Moore, Katie Moussouris, Peter G. Neumann, Hamed Okhravi, Jothy Rosenberg, Hamid Salim,Michael Siegel, Diane Strong, Gregory T. Sullivan, Richard Wang, Robert N. M. Watson, Guy Zyskind An MIT Connection Science and Engineering Book

Copyright: 55f4d389fb1c3e70dc691d15c671f011