Read Book Cyber Espionage E Cyber Counterintelligence Spionaggio E Controspionaggio Cibernetico Pdf File Free

Cyber espionage e cyber counterintelligence. Spionaggio e controspionaggio cibernetico Cyber Espionage e Cyber Counterintelligence *Reverse Deception: Organized Cyber Threat Counter-Exploitation* **ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015** *16th International Conference on Cyber Warfare and Security* **Cyber Weaponry ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and Security No Place to Hide 21st European Conference on Cyber Warfare and Security Public Information Management and E-Government** *Glass Houses* **Counterintelligence Theory and Practice America the Vulnerable** *ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security "* **ECCWS 2018 17th European Conference on Cyber Warfare and Security V2** *ECCWS 2020 20th European Conference on Cyber Warfare and Security* **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities** Cyber Security and Policy **Psychosocial Dynamics of Cyber Security National Security Intelligence and Ethics** *Report of the Redmond Panel* Deter, Disrupt, or Deceive **Discerning President Obama's National Security Strategy** *ECCWS 2021 20th European Conference on Cyber Warfare and Security* **US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale** *Cybercrime: An Encyclopedia of Digital Crime* The External Dimension of the European Union's Critical Infrastructure Protection Programme *107-1 Hearing: Energy And Water Development Appropriations For 2002, Part 5, 2001* **U.S. Department of Energy Performance and Accountability Report: Fiscal Year 2000** US Counterterrorism Activities Handbook Volume 1 Strategy, Operations, Programs **Cyber Espionage and International Law** *Energy and Water Development Appropriations for 2002* **Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century** ICCWS 2017 12th International Conference on Cyber Warfare and Security Energy and Water Development Appropriations for 2002: Secretary of Energy ... pt.6. Atomic Energy Defense activities ... pt.7. Testimony of members of Congress and other interested individual and organizations *ECCWS 2017 16th European Conference on Cyber Warfare and Security* *Cyber Warfare: A Documentary and Reference Guide* Protecting the Force **Weaknesses in Classified Information Security Controls at DOE's Nuclear Weapon Laboratories**

ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015 Nov 17 2022 Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited

Discerning President Obama's National Security Strategy Mar 29 2021 Volume 111 of Terrorism: Commentary on Security Documents, Discerning President Obama's National Security Strategy, makes available documents from the first fifteen months of the Obama administration that provide insights into its developing national security strategy. Included are documents that include detailed intelligence estimates and strategies as well as documents that outline important lessons regarding stability and reconstruction in Iraq. Additional documents provide valuable insight into the Obama Administration's Afghanistan and Pakistan Strategy. General Editor Douglas Lovelace, an expert in U.S. military matters, elucidates the complexities of military spending and of counter-insurgency tactics.

U.S. Department of Energy Performance and Accountability Report: Fiscal Year 2000 Aug 22 2020

Counterintelligence Theory and Practice Mar 09 2022 Designed for university students in the burgeoning field of intelligence studies and professional training classes, Counterintelligence Theory and Practice provides all the elements required for a successful counterintelligence operation. Exploring issues relating to national security, military, law enforcement, as well as corporate private affairs, Hank Prunckun uses his experience as a professional to explain both the theoretical basis and practical application for real counterintelligence craft. Each chapter contains key words and phrases and a number of study questions and learning activities that make the book a comprehensive tool for learning how to be a counterintelligence professional.

National Security Intelligence and Ethics Jul 01 2021 This volume examines the ethical issues that arise as a result of national security intelligence collection and analysis. Powerful new technologies enable the collection, communication, and analysis of national security data on an unprecedented scale. Data collection now plays a central role in intelligence practice, yet this development raises a host of ethical and national security problems, such as: privacy; autonomy; threats to national security and democracy by foreign states; and accountability for liberal democracies. This volume provides a comprehensive set of in-depth ethical analyses of these problems by combining contributions from both ethics scholars and intelligence practitioners. It provides the reader with a practical understanding of relevant operations, the issues that they raise, and analysis of how responses to these issues can be informed by a commitment to liberal democratic values. This combination of perspectives is crucial in providing an informed appreciation of ethical challenges that is also grounded in the realities of the practice of intelligence. This book will be of great interest to all students of intelligence studies, ethics, security studies, foreign policy, and International Relations.

16th International Conference on Cyber Warfare and Security Oct 16 2022 These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.

Cyber Security and Policy Sep 03 2021 A world without the advantages and convenience provided by cyberspace and the internet of things is now unimaginable. But do we truly grasp the threats to this massive, interconnected system? And do we really understand

how to secure it? After all, cyber security is no longer just a technology problem; the effort to secure systems and society are now one and the same. This book discusses cyber security and cyber policy in an effort to improve the use and acceptance of security services. It argues that a substantive dialogue around cyberspace, cyber security and cyber policy is critical to a better understanding of the serious security issues we face.

Energy and Water Development Appropriations for 2002 May 19 2020

Energy and Water Development Appropriations for 2002: Secretary of Energy ... pt.6. Atomic Energy Defense activities ... pt.7. Testimony of members of Congress and other interested individual and organizations Feb 14 2020

Cyber espionage e cyber counterintelligence. Spionaggio e controspionaggio cibernetico Feb 20 2023

ECCWS 2021 20th European Conference on Cyber Warfare and Security Feb 25 2021 Conferences Proceedings of 20th European Conference on Cyber Warfare and Security

No Place to Hide Jul 13 2022 A groundbreaking look at the NSA surveillance scandal, from the reporter who broke the story, Glenn Greenwald, star of Citizenfour, the Academy Award-winning documentary on Edward Snowden In May 2013, Glenn Greenwald set out for Hong Kong to meet an anonymous source who claimed to have astonishing evidence of pervasive government spying and insisted on communicating only through heavily encrypted channels. That source turned out to be the 29-year-old NSA contractor and whistleblower Edward Snowden, and his revelations about the agency's widespread, systemic overreach proved to be some of the most explosive and consequential news in recent history, triggering a fierce debate over national security and information privacy. As the arguments rage on and the government considers various proposals for reform, it is clear that we have yet to see the full impact of Snowden's disclosures. Now for the first time, Greenwald fits all the pieces together, recounting his high-intensity ten-day trip to Hong Kong, examining the broader implications of the surveillance detailed in his reporting for The Guardian, and revealing fresh information on the NSA's unprecedented abuse of power with never-before-seen documents entrusted to him by Snowden himself. Going beyond NSA specifics, Greenwald also takes on the establishment media, excoriating their habitual avoidance of adversarial reporting on the government and their failure to serve the interests of the people. Finally, he asks what it means both for individuals and for a nation's political health when a government pries so invasively into the private lives of its citizens—and considers what safeguards and forms of oversight are necessary to protect democracy in the digital age. Coming at a landmark moment in American history, No Place to Hide is a fearless, incisive, and essential contribution to our understanding of the U.S. surveillance state.

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities Oct 04 2021 The United States is increasingly dependent on information and information technology for both civilian and military purposes, as are many other nations. Although there is a substantial literature on the potential impact of a cyberattack on the societal infrastructure of the United States, little has been written about the use of cyberattack as an instrument of U.S. policy. Cyberattacks-actions intended to damage adversary computer systems or networks-can be used for a variety of military purposes. But they also have application to certain missions of the intelligence community, such as covert action. They may be useful for certain domestic law enforcement purposes, and some analysts believe that they might be useful for certain private sector entities who are themselves under cyberattack. This report considers all of these applications from an integrated perspective that ties together technology, policy, legal, and ethical issues. Focusing on the use of cyberattack as an instrument of U.S. national policy, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities explores important characteristics of cyberattack. It describes the current international and domestic legal structure as it might apply to cyberattack, and considers analogies to other domains of conflict to develop relevant insights. Of special interest to the military, intelligence, law enforcement, and homeland security communities, this report is also an essential point of departure for nongovernmental researchers interested in this rarely discussed topic.

107-1 Hearing: Energy And Water Development Appropriations For 2002, Part 5, 2001 Sep 22 2020

Protecting the Force Nov 12 2019 On Nov. 5, 2010, a gunman opened fire at the Soldier Readiness Center at Fort Hood, Texas. Thirteen people were killed and 43 others were wounded or injured. Following the shooting, Defense Sec. Robert M. Gates established the Dept. of Defense Independent Review Related to Fort Hood to address questions about the degree to which the entire Dept. is prepared for similar incidents in the future -- especially multiple, simultaneous incidents. This report includes, but is not limited to: identifying and monitoring potential threats; providing time-critical information to the right people; employing force protection measures; and planning for and responding to incidents.

Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century Apr 17 2020 Explaining cybercrime in a highly networked world, this book provides a comprehensive yet accessible summary of the history, modern developments, and efforts to combat cybercrime in various forms at all levels of government—international, national, state, and local. • Provides accessible, comprehensive coverage of a complex topic that encompasses identity theft to copyright infringement written for non-technical readers • Pays due attention to important elements of cybercrime that have been largely ignored in the field, especially politics • Supplies examinations of both the domestic and international efforts to combat cybercrime • Serves an ideal text for first-year undergraduate students in criminal justice programs

Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale Dec 26 2020 1360.31

ECCWS 2017 16th European Conference on Cyber Warfare and Security Jan 15 2020

ECCWS 2020 20th European Conference on Cyber Warfare and Security Nov 05 2021 These proceedings represent the work of contributors to the 19th European Conference on Cyber Warfare and Security (ECCWS 2020), supported by University of Chester, UK on 25-26 June 2020. The Conference Co-chairs are Dr Thaddeus Eze and Dr Lee Speakman, both from University of Chester and the Programme Chair is Dr Cyril Onwubiko from IEEE and Director, Cyber Security Intelligence at Research Series Limited. ECCWS is a well-established event on the academic research calendar and now in its 19th year the key aim remains the opportunity for participants to share ideas and meet. The conference was due to be held at University of Chester, UK, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will ensure an interesting conference. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

Glass Houses Apr 10 2022 A chilling and revelatory appraisal of the new faces of espionage and warfare on the digital battleground Shortly after 9/11, Joel Brenner entered the inner sanctum of American espionage, first as the inspector general of the National

Security Agency, then as the head of counterintelligence for the director of National Intelligence. He saw at close range the battleground on which adversaries are attacking us: cyberspace. Like the rest of us, governments and corporations inhabit “glass houses,” all but transparent to a new generation of spies who operate remotely from such places as China, the Middle East, Russia, and even France. In this urgent wake-up call, Brenner draws on his extraordinary background to show what we can—and cannot—do to prevent cyber spies and hackers from compromising our security and stealing our latest technology.

Psychosocial Dynamics of Cyber Security Aug 02 2021 This new volume, edited by industrial and organizational psychologists, will look at the important topic of cyber security work in the US and around the world. With contributions from experts in the fields of industrial and organizational psychology, human factors, computer science, economics, and applied anthropology, the book takes the position that employees in cyber security professions must maintain attention over long periods of time, must make decisions with imperfect information with the potential to exceed their cognitive capacity, may often need to contend with stress and fatigue, and must frequently interact with others in team settings and multiteam systems. Consequently, psychosocial dynamics become a critical driver of cyber security effectiveness. Chapters in the book reflect a multilevel perspective (individuals, teams, multiteam systems) and describe cognitive, affective and behavioral inputs, processes and outcomes that operate at each level. The book chapters also include contributions from both research scientists and cyber security policy-makers/professionals to promote a strong scientist-practitioner dynamic. The intent of the book editors is to inform both theory and practice regarding the psychosocial dynamics of cyber security work.

The External Dimension of the European Union’s Critical Infrastructure Protection Programme Oct 24 2020 External Dimension of the European Union’s Critical Infrastructure Protection Programme: From Neighboring Frameworks to Transatlantic Cooperation provides the basis, methodological framework, and first comprehensive analysis of the current state of the external dimension European Programme for Critical Infrastructure Protection. The challenges at the EU level are multidimension insofar as identifying, designating and protecting critical infrastructures with the ultimate goal of harmonizing different national policies of the Member States and creating the identity of the European Union in this arena. Modern society has become so reliant on various sectors of critical infrastructure—energy, telecommunications, transport, finance, ICT, and public services—that any disruption may lead to serious failures that impact individuals, society, and the economy. The importance of critical infrastructures grows with the industrial development of global and national communities; their interdependence and resiliency is increasingly important given security threats including terrorism, natural disaster, climate change and pandemic outbreak In the area of Critical Infrastructure Protection and Resilience, the European Union is constantly committed to setting the objectives for the Member States. At the same time, the European Commission promotes the importance of a common approach to Critical Infrastructure Protection (CIP), and ensure cooperation beyond the borders of the Union, while also cooperating with neighboring countries, including those soon willing to join the European Union. This book has been structured and written to contribute to current critical infrastructures, resilience policy development and discussions about regional and international cooperation. It serves as a reference for those countries willing to initiate cooperation and that therefore demand deeper knowledge on the security cultures and frameworks of their potential partners. Features: Provides an unprecedented analysis of the national frameworks of 14 neighboring countries of the EU, plus the United States and Canada Overcomes the language barriers to provide an overall picture of the state of play of the countries considered Outlines the shaping of national critical infrastructure protection frameworks to understanding the importance of service stability and continuity Presents guidelines to building a comprehensive and flexible normative framework Addresses the strategic and operational importance of international co-operation on critical infrastructure including efforts in CIP education and training Provides insight to institutions and decision-makers on existing policies and ways to improve the European security agenda The book explains and advocates for establishing stronger, more resilient systems to preserve functionalities at the local, national, and international levels. Security, industry, and policy experts—both practitioners and policy decision-makers—looking for answers will find the solutions they seek within this book.

Public Information Management and E-Government May 11 2022 Recently, the public sector has given an increasing amount of national and international attention to electronic government systems. Therefore, it is inevitable that the theoretical implications and intersections between information technology and governmental matters are more widely discussed. Public Information Management and E-Government: Policy and Issues offers a fresh, comprehensive dialogue on issues that occur between the public management and information technology domains. With its focus on political issues and their effects on the larger public sector, this book is valuable for administrators, researchers, students, and educators who wish to gain foundational and theoretical knowledge on e-government policies.

Weaknesses in Classified Information Security Controls at DOE's Nuclear Weapon Laboratories Oct 12 2019

US Counterterrorism Activities Handbook Volume 1 Strategy, Operations, Programs Jul 21 2020 2011 Updated Reprint. Updated Annually. US Anti Terrorism Handbook: Strategy, Operations, Programs

ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and Security Aug 14 2022

Report of the Redmond Panel May 31 2021

America the Vulnerable Feb 08 2022 Now available in a new edition entitled GLASS HOUSES: Privacy, Secrecy, and Cyber Insecurity in a Transparent World. A former top-level National Security Agency insider goes behind the headlines to explore America's next great battleground: digital security. An urgent wake-up call that identifies our foes; unveils their methods; and charts the dire consequences for government, business, and individuals. Shortly after 9/11, Joel Brenner entered the inner sanctum of American espionage, first as the inspector general of the National Security Agency, then as the head of counterintelligence for the director of national intelligence. He saw at close range the battleground on which our adversaries are now attacking us-cyberspace. We are at the mercy of a new generation of spies who operate remotely from China, the Middle East, Russia, even France, among many other places. These operatives have already shown their ability to penetrate our power plants, steal our latest submarine technology, rob our banks, and invade the Pentagon's secret communications systems. Incidents like the WikiLeaks posting of secret U.S. State Department cables hint at the urgency of this problem, but they hardly reveal its extent or its danger. Our government and corporations are a "glass house," all but transparent to our adversaries. Counterfeit computer chips have found their way into our fighter aircraft; the Chinese stole a new radar system that the navy spent billions to develop; our own soldiers used intentionally corrupted thumb drives to

download classified intel from laptops in Iraq. And much more. Dispatches from the corporate world are just as dire. In 2008, hackers lifted customer files from the Royal Bank of Scotland and used them to withdraw $9 million in half an hour from ATMs in the United States, Britain, and Canada. If that was a traditional heist, it would be counted as one of the largest in history. Worldwide, corporations lose on average $5 million worth of intellectual property apiece annually, and big companies lose many times that. The structure and culture of the Internet favor spies over governments and corporations, and hackers over privacy, and we've done little to alter that balance. Brenner draws on his extraordinary background to show how to right this imbalance and bring to cyberspace the freedom, accountability, and security we expect elsewhere in our lives. In America the Vulnerable, Brenner offers a chilling and revelatory appraisal of the new faces of war and espionage-virtual battles with dangerous implications for government, business, and all of us.
Cyber Weaponry Sep 15 2022 There is little doubt that cyber-space has become the battle space for confrontations. However, to conduct cyber operations, a new armory of weapons needs to be employed. No matter how many, or how sophisticated an aggressor's kinetic weapons are, they are useless in cyber-space. This book looks at the milieu of the cyber weapons industry, as well as the belligerents who use cyber weapons. It discusses what distinguishes these hardware devices and software programs from computer science in general. It does this by focusing on specific aspects of the topic—contextual issues of why cyber-space is the new battleground, defensive cyber weapons, offensive cyber weapons, dual-use weapons, and the implications these weapons systems have for practice. Contrary to popular opinion, the use of cyber weapons is not limited to nation states; though this is where the bulk of news reporting focuses. The reality is that there isn't a sector of the political-economy that is immune to cyber skirmishes. So, this book looks at cyber weapons not only by national security agencies and the military, but also by law enforcement, and the business sector—the latter includes administrations termed non-government organisations (NGOs). This book offers study material suitable for a wide-ranging audience—students, professionals, researchers, policy officers, and ICT specialists.
ICCWS 2017 12th International Conference on Cyber Warfare and Security Mar 17 2020
Cyber Warfare: A Documentary and Reference Guide Dec 14 2019 Providing an invaluable introductory resource for students studying cyber warfare, this book highlights the evolution of cyber conflict in modern times through dozens of key primary source documents related to its development and implementation. This meticulously curated primary source collection is designed to offer a broad examination of key documents related to cyber warfare, covering the subject from multiple perspectives. The earliest documents date from the late 20th century, when the concept and possibility of cyber attacks became a reality, while the most recent documents are from 2019. Each document is accompanied by an introduction and analysis written by an expert in the field that provides the necessary context for readers to learn about the complexities of cyber warfare. The title's nearly 100 documents are drawn primarily but not exclusively from government sources and allow readers to understand how policy, strategy, doctrine, and tactics of cyber warfare are created and devised, particularly in the United States. Although the United States is the global leader in cyber capabilities and is largely driving the determination of norms within the cyber domain, the title additionally contains a small number of international documents. This invaluable work will serve as an excellent starting point for anyone seeking to understand the nature and character of international cyber warfare. Covers in detail one of the defining forms of conflict of the 21st century—cyber warfare will significantly impact virtually every American citizen over the next two decades Provides more than 90 primary source documents and matching analysis, allowing readers to investigate the underpinnings of cyber warfare Enables readers to see the development of different concepts of cyber warfare through its chronological organization Reflects the deep knowledge of an editor who is a noted expert in cyber warfare and has taught for the United States Air Force for more than a decade
Reverse Deception: Organized Cyber Threat Counter-Exploitation Dec 18 2022 In-depth counterintelligence tactics to fight cyber-espionage "A comprehensive and unparalleled overview of the topic by experts in the field."--Slashdot Expose, pursue, and prosecute the perpetrators of advanced persistent threats (APTs) using the tested security techniques and real-world case studies featured in this one-of-a-kind guide. Reverse Deception: Organized Cyber Threat Counter-Exploitation shows how to assess your network's vulnerabilities, zero in on targets, and effectively block intruders. Discover how to set up digital traps, misdirect and divert attackers, configure honeypots, mitigate encrypted crimeware, and identify malicious software groups. The expert authors provide full coverage of legal and ethical issues, operational vetting, and security team management. Establish the goals and scope of your reverse deception campaign Identify, analyze, and block APTs Engage and catch nefarious individuals and their organizations Assemble cyber-profiles, incident analyses, and intelligence reports Uncover, eliminate, and autopsy crimeware, trojans, and botnets Work with intrusion detection, anti-virus, and digital forensics tools Employ stealth honeynet, honeypot, and sandbox technologies Communicate and collaborate with legal teams and law enforcement
US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments Jan 27 2021 US National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments
21st European Conference on Cyber Warfare and Security Jun 12 2022
Cyber Espionage and International Law Jun 19 2020 The advent of cyberspace has led to a dramatic increase in state-sponsored political and economic espionage. This monograph argues that these practices represent a threat to the maintenance of international peace and security and assesses the extent to which international law regulates this conduct. The traditional view among international legal scholars is that, in the absence of direct and specific international law on the topic of espionage, cyber espionage constitutes an extra-legal activity that is unconstrained by international law. This monograph challenges that assumption and reveals that there are general principles of international law as well as specialised international legal regimes that indirectly regulate cyber espionage. In terms of general principles of international law, this monograph explores how the rules of territorial sovereignty, non-intervention and the non-use of force apply to cyber espionage. In relation to specialised regimes, this monograph investigates the role of diplomatic and consular law, international human rights law and the law of the World Trade Organization in addressing cyber espionage. This monograph also examines whether developments in customary international law have carved out espionage exceptions to those international legal rules that otherwise prohibit cyber espionage as well as considering whether the doctrines of self-defence and necessity can be invoked to justify cyber espionage. Notwithstanding the applicability of international law, this monograph concludes that policymakers should nevertheless devise an international law of espionage which, as lex specialis, contains rules that are specifically designed to confront the growing threat posed by cyber espionage.
Cybercrime: An Encyclopedia of Digital Crime Nov 24 2020 This important reference work is an extensive, up-to-date resource for

students wanting to immerse themselves in the world of cybercrime, or for those seeking further knowledge of specific attacks both domestically and internationally. Cybercrime is characterized by criminal acts that take place in the borderless digital realm. It takes on many forms, and its perpetrators and victims are varied. From financial theft, destruction of systems, fraud, corporate espionage, and ransoming of information to the more personal, such as stalking and web-cam spying as well as cyberterrorism, this work covers the full spectrum of crimes committed via cyberspace. This comprehensive encyclopedia covers the most noteworthy attacks while also focusing on the myriad issues that surround cybercrime. It includes entries on such topics as the different types of cyberattacks, cybercrime techniques, specific cybercriminals and cybercrime groups, and cybercrime investigations. While objective in its approach, this book does not shy away from covering such relevant, controversial topics as Julian Assange and Russian interference in the 2016 U.S. presidential election. It also provides detailed information on all of the latest developments in this constantly evolving field. Includes an introductory overview essay that discusses all aspects of cybercrime—how it's defined, how it developed, and its massive expansion in recent years Offers a wide array of entries regarding cybercrime and the many ways it can be committed Explores the largest, most costly cyber attacks on a variety of victims, including corporations, governments, consumers, and individuals Provides up-to-date information on the ever-evolving field of cybercrime

Cyber Espionage e Cyber Counterintelligence Jan 19 2023

ECCWS 2018 17th European Conference on Cyber Warfare and Security V2 Dec 06 2021

*ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security "*Jan 07 2022 These proceedings represent the work of researchers participating in the 15th European Conference on Cyber Warfare and Security (ECCWS 2016) which is being hosted this year by the Universitat der Bundeswehr, Munich, Germany on the 7-8 July 2016. ECCWS is a recognised event on the International research conferences calendar and provides a valuable plat-form for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyberwar and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and ex-panding range of Cyberwar and Cyber Security research available to them. With an initial submission of 110 abstracts, after the double blind, peer review process there are 37 Academic research papers and 11 PhD research papers, 1 Master's research paper, 2 Work In Progress papers and 2 non-academic papers published in these Conference Proceedings. These papers come from many different coun-tries including Austria, Belgium, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, Ireland, Kenya, Luxembourg, Netherlands, Norway, Portugal, Romania, Russia, Slovenia, South Africa, Sweden, Turkey, UK and USA. This is not only highlighting the international character of the conference, but is also promising very interesting discussions based on the broad treasure trove of experience of our community and partici-pants."

Deter, Disrupt, or Deceive Apr 29 2021 A fresh perspective on statecraft in the cyber domain The idea of “cyber war” has played a dominant role in both academic and popular discourse concerning the nature of statecraft in the cyber domain. However, this lens of war and its expectations for death and destruction may distort rather than help clarify the nature of cyber competition and conflict. Are cyber activities actually more like an intelligence contest, where both states and nonstate actors grapple for information advantage below the threshold of war? In Deter, Disrupt, or Deceive, Robert Chesney and Max Smeets argue that reframing cyber competition as an intelligence contest will improve our ability to analyze and strategize about cyber events and policy. The contributors to this volume debate the logics and implications of this reframing. They examine this intelligence concept across several areas of cyber security policy and in different national contexts. Taken as a whole, the chapters give rise to a unique dialogue, illustrating areas of agreement and disagreement among leading experts and placing all of it in conversation with the larger fields of international relations and intelligence studies. Deter, Disrupt, or Deceive is a must read because it offers a new way for scholars, practitioners, and students to understand statecraft in the cyber domain.