Cyber Reconnaissance Surveillance And Defense

At a time when online surveillance and cybercrime techniques are widespread, and are being used by governments, corporations, and individuals, Cyber Reconnaissance, Surveillance and Defense gives you a practical resource that explains how these activities are being carried out and shows how to defend against them. Expert author Rob Shimonski shows you how to carry out advanced IT surveillance and reconnaissance, describes when and how these techniques are used, and provides a full legal background for each threat. To help you understand how to defend against these attacks, this book describes many new and leading-edge surveillance, information-gathering, and personal exploitation threats taking place today, including Web cam breaches, home privacy systems, physical and logical tracking, phone tracking, picture metadata, physical device tracking and geo-location, social media security, identity theft, social engineering, sniffing, and more. Understand how IT surveillance and reconnaissance techniques are being used to track and monitor activities of individuals and organizations Find out about the legal basis of these attacks and threats — what is legal and what is not — and how to defend against any type of surveillance Learn how to thwart monitoring and surveillance threats with practical tools and techniques Real-world examples teach using key concepts from cases in the news around the world

This edited volume argues that producers of analysis need to shift from producing static, narrative products to much more dynamic, digitally-based platforms in order to remain competitive and relevant.

Cyber weapons and the possibility of cyber conflict—including interference in foreign political campaigns, industrial sabotage, attacks on infrastructure, and combined military campaigns—require policymakers, scholars, and citizens to rethink twenty-first-century warfare. Yet because cyber capabilities are so new and continually developing, there is little agreement about how they will be deployed, how effective they can be, and how they can be managed. Written by leading scholars, the fourteen case studies in this volume will help policymakers, scholars, and students make sense of contemporary cyber conflict through historical analogies to past military-technological problems. The chapters are divided into three groups. The first—What Are Cyber Weapons Like?—examines the characteristics of cyber capabilities and how their use for intelligence gathering, signaling, and precision striking compares with earlier technologies for such missions. The second section—What Might Cyber Wars Be Like?—explores how lessons from several wars since the early nineteenth century, including the World Wars, could apply—or not—to cyber conflict in the twenty-first century. The final section—What Is Preventing and/or Managing Cyber Conflict Like?—offers lessons from past cases of managing threatening actors and technologies.

In today's society, cyberspace is at the heart of daily living and is both a gift and a burden. The United States is taking measures to ensure that cyberspace continues to be a gift to the population. However, those measures can be a burden on those implementing them if the underlying command and control is immature or complex. The Department of Defense (DOD) has taken a proactive approach to viewing cyberspace as a battlefield and engaging in its defense. The U.S. Strategic Command (USSTRATCOM) has DOD command and control over cyberspace and has delegated much of that to the Defense Information Systems Agency (DISA) Joint Task Force - Global Network Operations (JTF-GNO) for every day global network operations. The Geographic Combatant Commander (CCDR) is responsible for computer network operations within the Geographic Combatant Command (GCC) area of responsibility. The CCDR uses a Theater Network Operations Control Center (TNCC) to oversee network operations in the theater. JTF-GNO has forward deployed assets in GCC known as a Theater Network Operations Center (TNC) which provide the CCDR with the Global Information Grid (GIG) situational awareness within the theater relative to the global view. USEUCOM has taken its defense of its cyberspace assets one step further by creating a Cyber-Threat Intelligence Cell to characterize current threats with the intent to proactively prevent cyber attacks. The CCDR has many options available to successfully protect and defend the GCC cyberspace assets, but these options can be complex and insufficient. This paper compares and contrasts current theater structures and relationships and recommends a course of action for the CCDR to proactively and effectively protect and defend theater cyberspace assets.

Cyber Warfare

Reverse Deception: Organized Cyber Threat Counter-Exploitation

Techniques, Tactics and Tools for Security Practitioners

Howard F. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015

Strategy and Responses

Report of the Committee on Armed Services, House of Representatives on H.R. 4435 Together with Additional Views (including Cost Estimate of the Congressional Budget Office).

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.

Advanced Persistent Security covers secure network design and implementation, including authentication, authorization, data and access integrity, network monitoring, and risk assessment. Using such recent high profile cases as Target, Sony, and Home Depot, the book explores information security risks, identifies the common threats organizations face, and presents tactics on how to prioritize the right countermeasures. The book discusses concepts such as malignant versus malicious

threats, adversary mentality, motivation, the economics of cybercrime, the criminal infrastructure, dark webs, and the criminals organizations currently face. Contains practical and cost-effective recommendations for proactive and reactive protective measures Teaches users how to establish a viable threat intelligence program Focuses on how social networks present a double-edged sword against security programs

In response to a tasking from the Air Force chief of staff, the Air Force Research Institute conducted a review of how the Air Force organizes, educates/trains, and equips its cyber workforce. The resulting findings were used to develop recommendations for how the Air Force should recruit, educate, train, and develop cyber operators from the time they are potential accessions until they become senior leaders in the enlisted and officer corps. This study's discoveries, analyses, and recommendations are aimed at guiding staff officers and senior leaders alike as they consider how to develop a future cyber workforce that supports both Air Force and US Cyber Command missions across the range of military operations.

Hybrid conflicts are characterized by multi-layered efforts to undermine the functioning of the State or polarize society. This book presents results, recommendations and best practices from the NATO Advanced Research Workshop (ARW) "Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges", held in Stockholm, Sweden, in May 2016. The main objective of this workshop was to help and support NATO in the field of hybrid conflicts by developing a set of tools to deter and defend against adversaries mounting a hybrid offensive. Addressing the current state of critical infrastructure protection (CIP) and the challenges evolving in the region due to non-traditional threats which often transcend national borders – such as cyber attacks, terrorism, and attacks on energy supply – the widely ranging group of international experts who convened for this workshop provided solutions from a number of perspectives to counter the new and emerging challenges affecting the security of modern infrastructure. Opportunities for public-private partnerships in NATO member and partner countries were also identified. The book provides a highly topical resource which identifies common solutions for combating major hazards and challenges – namely cyber attacks, terrorist attacks on energy supply, man-made disasters, information warfare and maritime security risks – and will be of interest to all those striving to maintain stability and avoid adverse effects on the safety and well-being of society.

Airpower Lessons for an Air Force

The Rise of the Military-Internet Complex

Proliferation of Weapons- and Dual-Use Technologies

Developments and Advances in Defense and Security

Protecting Critical Infrastructure at the State and Local Level

Human Rights Responsibilities in the Digital Age

The Evolving Character of Power and Coercion

How rival states employ cyber strategy : disruption, espionage, and degradation -- The correlates of cyber strategy -- Cyber coercion as a combined strategy -- Commissars and crooks : Russian cyber coercion -- China and the technology gap : Chinese strategic behavior in cyberspace -- The United States : the cyber reconnaissance-strike complex

The conduct of warfare is constantly shaped by new forces that create complexities in the battlespace for military operations. As the nature of how and where wars are fought changes, new challenges to the application of the extant body of international law that regulates armed conflicts arise. This inaugural volume of the Lieber Studies Series seeks to address several issues in the confluence of law and armed conflict, with the primary goal of providing the reader with both academic and practitioner perspectives. Featuring chapters from world class scholars, policymakers and other government officials; military and civilian legal practitioners; and other thought leaders, together they examine the role of the law of armed conflict in current and future armed conflicts around the world. Complex Battlespaces also explores several examples of battlespace dynamics through four "lenses of complexity": complexity in legal regimes, governance, technology, and the urbanization of the battlefield.

The Wireshark Field Guide provides hackers, pen testers, and network administrators with practical guidance on capturing and interactively browsing computer network traffic. Wireshark is the world's foremost network protocol analyzer, with a rich feature set that includes deep inspection of hundreds of protocols, live capture, offline analysis and many other features. The Wireshark Field Guide covers the installation, configuration and use of this powerful multi-platform tool. The book give readers the hands-on skills to be more productive with Wireshark as they drill down into the information contained in real-time network traffic. Readers will learn the fundamentals of packet capture and inspection, the use of color codes and filters, deep analysis, including probes and taps, and much more. The Wireshark Field Guide is an indispensable companion for network technicians, operators, and engineers. Learn the fundamentals of using Wireshark in a concise field manual Quickly create functional filters that will allow you to get to work quickly on solving problems Understand the myriad of options and the deep functionality of Wireshark Solve common network problems Learn some advanced features, methods and helpful ways to work more quickly and efficiently

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

The Law of Armed Conflict and the Dynamics of Modern Warfare

Fact Or Fiction: Internet Surveillance and Reconnaissance Cell

Spies, Lies, and Algorithms

Department of Defense Dictionary of Military and Associated Terms

Analyzing and Troubleshooting Network Traffic

Introduction to Cyber-Warfare

Beyond Intrusion Detection

Unmanned Aircraft Systems (UAS) are an integral part of the US national critical infrastructure. They must be protected from hostile intent or use to the same level as any other military or commercial asset involved in US national security. However, from the Spratly Islands to Djibouti to heartland America, the expanding Chinese Unmanned Aircraft Systems (UAS / Drone) industry has outpaced the US technologically and numerically on all fronts: military, commercial, and recreational. Both countries found that there were large information security gaps in unmanned systems that could be exploited on the international cyber-security stage. Many of those gaps remain today and are direct threats to US advanced Air Assets if not mitigated upfront by UAS designers and manufacturers. The authors contend that US military / commercial developers of UAS hardware and software must perform cyber risk assessments and mitigations prior to delivery of UAS systems to stay internationally competitive and secure. The authors have endeavored to bring a breadth and quality of information to the reader that is unparalleled in the unclassified sphere. This book will fully immerse and engage the reader in the cyber-security considerations of this rapidly emerging technology that we know as unmanned aircraft systems (UAS). Topics covered include National Airspace (NAS) policy issues, information security, UAS vulnerabilities in key systems (Sense and Avoid / SCADA), collision avoidance systems, stealth design, intelligence, surveillance and reconnaissance (ISR) platforms; weapons systems security; electronic warfare considerations; data-links, jamming operational vulnerabilities and still-emerging political scenarios that affect US military / commercial decisions.

The aim of the book is to analyse and understand the impacts of artificial intelligence in the fields of national security and defense; to identify the political, geopolitical, strategic issues of AI; to analyse its place in conflicts and cyberconflicts, and more generally in the various forms of violence; to explain the appropriation of artificial intelligence by military organizations, but also law enforcement agencies and the police; to discuss the questions that the development of artificial intelligence and its use raise in armies, police, intelligence agencies, at the tactical, operational and strategic levels.

What people are saying about Inside Cyber Warfare "The necessary handbook for the 21st century." --Lewis Shepherd, Chief Tech Officer and Senior Fellow, Microsoft Institute for Advanced Technology in Governments "A must-read for policy makers and leaders who need to understand the big-picture landscape of cyber war." --Jim Stogdill, CTO, Mission Services Accenture You may have heard about "cyber warfare" in the news, but do you really know what it is? This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Inside Cyber Warfare goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside multiple cyber-conflicts that occurred from 2002 through summer 2009. Learn how cyber attacks are waged in open conflicts, including recent hostilities between Russia and Georgia, and Israel and Palestine Discover why Twitter, Facebook, LiveJournal, Vkontakte, and other sites on the social web are mined by the intelligence services of many nations Read about China's commitment to penetrate the networks of its technologically superior adversaries as a matter of national survival Find out why many attacks originate from servers in the United States, and who's responsible Learn how hackers are "weaponizing" malware to attack vulnerabilities at the application

level

This book examines the tangled responsibilities of states, companies, and individuals surrounding human rights in the digital age. Digital technologies have a huge impact – for better and worse – on human lives; while they can clearly enhance some human rights, they also facilitate a wide range of violations. States are expected to implement efficient measures against powerful private companies, but, at the same time, they are drawn to technologies that extend their own control over citizens. Tech companies are increasingly asked to prevent violations committed online by their users, yet many of their business models depend on the accumulation and exploitation of users' personal data. While civil society has a crucial part to play in upholding human rights, it is also the case that individuals harm other individuals online. All three stakeholders need to ensure that technology does not provoke the disintegration of human rights. Bringing together experts from a range of disciplines, including law, international relations, and journalism, this book provides a detailed analysis of the impact of digital technologies on human rights, which will be of interest to academics, research students and professionals concerned by this issue.

Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018)

The Human Side of Cyber Conflict- Organizing, Training and Equipping the Air Force Cyber Workforce

Cyber-Power Targeting Theory

A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies

Cyber-Physical Security

Evolving Intelligence, Surveillance and Reconnaissance (ISR) for Air Force Cyber Defense

@WAR

Cyber Warfare Techniques, Tactics and Tools for Security Practitioners provides a comprehensive look at how and why digital warfare is waged. This book explores the participants, battlefields, and the tools and techniques used during today's digital conflicts. The concepts discussed will give students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. Every one of our systems is under attack from multiple vectors - our defenses must be ready all the time and our alert systems must detect the threats every time. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It considers relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Starting with a definition of cyber warfare, the book ' s 15 chapters discuss the following topics: the cyberspace battlefield; cyber doctrine; cyber warriors; logical, physical, and psychological weapons; computer network exploitation; computer network attack and defense; non-state actors in computer network operations; legal system impacts; ethics in cyber warfare; cyberspace challenges; and the future of cyber war. This book is a valuable resource to those involved in cyber warfare activities, including policymakers, penetration testers, security professionals, network and systems administrators, and college instructors. The information provided on cyber tactics and attacks can also be used to assist in developing improved and more efficient procedures and technical defenses. Managers will find the text useful in improving the overall risk management strategies for their organizations. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result

This book creates a framework for understanding and using cyberpower in support of national security. Cyberspace and cyberpower are now critical elements of international security. United States needs a national policy which employs cyberpower to support its national security interests.

This book focuses on the vulnerabilities of state and local services to cyber-threats and suggests possible protective action that might be taken against such threats. Cyber-threats to U.S. critical infrastructure are of growing concern to policymakers, managers and consumers. Information and communications technology (ICT) is ubiquitous and many ICT devices and other components are interdependent; therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on the national security, the economy, and the livelihood and safety of many individual citizens. Traditionally cyber security has generally been viewed as being focused on higher level threats such as those against the internet or the Federal government. Little attention has been paid to cyber-security at the state and local level. However, these governmental units play a critical role in providing services to local residents and consequently are highly vulnerable to cyber-threats. The failure of these services, such as waste water collection and water supply, transportation, public safety, utility services, and communication services, would pose a great threat to the public. Featuring contributions from leading experts in the field, this volume is intended for state and local government officials and managers, state and Federal officials, academics, and public policy specialists.

Intelligence challenges in the digital age : Cloaks, daggers, and tweets -- The education crisis : How fictional spies are shaping public opinion and intelligence policy -- American intelligence history at a glance-from fake bakeries to armed drones -- Intelligence basics : Knowns and unknowns -- Why analysis is so hard : The seven deadly biases -- Counterintelligence : To catch a spy -- Covert action - "a hard business of agonizing choices" -- Congressional oversight : Eyes on spies -- Intelligence isn't just for governments anymore : Nuclear sleuthing in a Google earth world -- Decoding cyber threats.

Advanced Persistent Security

Mapping the Cyber Underworld

The Tao of Network Security Monitoring

States and Selves

Spaces of Surveillance
The Strategic Dimensions of Offensive Cyber Operations
The Basics of Hacking and Penetration Testing

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

Introduction to Cyber-Warfare: A Multidisciplinary Approach, written by experts on the front lines, gives you an insider's look into the world of cyber-warfare through the use of recent case studies. The book examines the issues related to cyber warfare not only from a computer science perspective but from military, sociological, and scientific perspectives as well. You'll learn how cyber-warfare has been performed in the past as well as why various actors rely on this new means of warfare and what steps can be taken to prevent it. Provides a multi-disciplinary approach to cyber-warfare, analyzing the information technology, military, policy, social, and scientific issues that are in play Presents detailed case studies of cyber-attack including inter-state cyber-conflict (Russia-Estonia), cyber-attack as an element of an information operations strategy (Israel-Hezbollah,) and cyber-attack as a tool against dissidents within a state (Russia, Iran) Explores cyber-attack conducted by large, powerful, non-state hacking organizations such as Anonymous and LulzSec Covers cyber-attacks directed against infrastructure, such as water treatment plants and power-grids, with a detailed account of Stuxent

In a world of ubiquitous surveillance, watching and being watched are the salient features of the lives depicted in many of our cultural productions. This collection examines surveillance as it is portrayed in art, literature, film and popular culture, and makes the connection between our sense of 'self' and what is 'seen'. In our post-panoptical world which purports to proffer freedom of movement, technology notes our movements and habits at every turn. Surveillance seeps out from businesses and power structures to blur the lines of security and confidentiality. This unsettling loss of privacy plays out in contemporary narratives, where the 'selves' we create are troubled by

surveillance. This collection will appeal to scholars of media and cultural studies, contemporary literature, film and art and American studies.
"Examines cyberspace threats and policies from the vantage points of China and the U.S"--
Strategic Cyber Security
Intelligence Communication in the Digital Era: Transforming Security, Defence and Business
The U.S. Cybersecurity and Intelligence Analysis Challenges
Bytes, Bombs, and Spies
The Wireshark Field Guide
Complex Battlespaces
Unmanned Aircraft Systems (Uas) in the Cyber Domain: Protecting Usa's Advanced Air Assets

This book explores and analyzes the rapid pace of technological evolution in diplomatic, information, military, and economic sectors, which has contributed to a dynamic international policy environment. Global political stability is greatly influenced by innovations originating from numerous sources, including university labs, the technology sector, and military research. Collectively, these innovations guide the movement of people, ideas, and technology that in turn affect the international balance of power. The objective of this volume is to develop new insights into how the proliferation of innovative ideas, low-cost weapons, and dual-use technologies impact the changing global security landscape. Innovative and dual-use technologies can be used for beneficial purposes or defensive purposes. Alternatively they may be appropriated or employed for nefarious purposes by hostile military powers and non-state actors alike. Such actions can threaten global security and stability. As the complexity of technological innovations continues to increase, existing control mechanisms such as international regulations and security arrangements may be insufficient to stem the tide of proliferation over time. As such, this works seeks to assess and present policy solutions to curtail the threat to global stability posed by the proliferation of weapons and dual-use technology.
At a time when online surveillance and cybercrime techniques are widespread, and are being used by governments, corporations, and individuals, Cyber Reconnaissance, Surveillance and Defense gives you a practical resource that explains how these activities are being carried out and shows how to defend against them. Expert author Rob Shimonski shows you how to carry out advanced IT surveillance and reconnaissance, describes when and how these techniques are used, and provides a full legal background for each threat. To help you understand how to defend against these attacks, this book describes many new and leading-edge surveillance, information-gathering, and personal exploitation threats taking place today, including Web cam breaches, home privacy systems, physical and logical tracking, phone tracking, picture metadata, physical device tracking and geo-location, social media security, identity theft, social engineering, sniffing, and more. Understand how IT surveillance and reconnaissance techniques are being used to track and monitor activities of individuals and organizations Find out about the legal basis of these attacks and threats - what is legal and what is not - and how to defend against any type of surveillance Learn how to thwart monitoring and surveillance threats with practical tools and techniques Real-world examples teach using key concepts from cases in the news around the world
This book includes a selection of articles from The 2018 Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS'18), held in Salinas, Peninsula de Santa Elena, Ecuador, from April 18 to 20, 2018. MICRADS is an international forum for researchers and practitioners to present and discuss the most recent innovations, trends, results, experiences and concerns in the various areas of defense and security, together with their technological development and applications. The main topics covered are: Information and Communication Technology in Education; Computer Vision in Military Applications; Engineering Analysis and Signal Processing; Cybersecurity and Cyberdefense; Maritime Security and Safety; Strategy, Geopolitics and Oceanopolitics; Defense planning; Leadership (e-leadership); Defense Economics; Defense Logistics; Health Informatics in Military Applications; Simulation in Military Applications; Computer Networks, Mobility and Pervasive Systems; Military Marketing; Military Physical Training; Assistive Devices and Wearable Technology; Naval and Military Engineering; Weapons and Combat Systems; Operational Oceanography. The book is aimed at all those dealing with defense and security issues, including practitioners, researchers and teachers as well as undergraduate, graduate, master's and doctorate students.
This report presents an open source analysis of North Korea's cyber operations capabilities and its strategic implications for the United States and South Korea. The purpose is to mitigate the current knowledge gap among various academic and policy communities on the topic by synthesizing authoritative and comprehensive open source reference material. The report is divided into three chapters, the first chapter examining North Korea's cyber strategy. The authors then provide an assessment of North Korea's cyber operations capabilities by examining the organizational structure, history, and functions of North Korea's cyber units, their supporting educational training and technology base, and past cyber attacks widely attributed to North Korea. This assessment is followed by a discussion on policy implications for U.S. and ROK policymakers and the larger security community.
China and Cybersecurity
Cyber Crime and Forensic Computing
Fourteen Analogies
Diplomatic, Information, Military, and Economic Approaches
States, Companies and Individuals
Is Cyber Deterrence Possible?
Inside Cyber Warfare

One of the prevailing issues regarding security to North America and more pointedly, the United States, gravitates on the topic of cyber threats confronting this nation. These threats are becoming more disruptive and destructive and many nations' infrastructure is vulnerable to them. This book makes use of a qualitative research methodology looking at a conventional understanding of the four instruments of power that include diplomacy, information, military and economic (D.I.M.E.) efforts through the use of the York Intelligence Red Team Model-Cyber (Modified) and seeing how adversaries are using them against the United States. Moreover, this project uses secondary data and makes use of the Federal Secondary Data Case Study Triangulation Model to ensure a

balance of sources to dissect the problem. John M. Weaver is Associate Professor of Intelligence Analysis at York College of Pennsylvania, the US.

"This paper provides several recommendations to advance ISR for cyber defense. The Air Force should develop a robust ISR Processing, Exploitation and Dissemination (PED) capability devoted to cyberspace. Additionally, the Air Force should conduct an in-depth study to determine resources required for the National Air and Space Intelligence Center to grow capacity for more robust analysis of adversary cyber capabilities. Next, a stronger cyber defensive strategy, enabled by ISR, will require additional intelligence resources or realignment of existing resources in the Air Force ISR Agency and 24th Air Force. ISR capabilities will be the catalyst for cyber defense of critical assets to more fully protect commanders' air, space and cyber operations."--Abstract.

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

An investigation into how the Pentagon, NSA, and other government agencies are uniting with corporations to fight in cyberspace, the next great theater of war.

Cyberpower and National Security

Modern Principles, Practices, and Algorithms

Artificial Intelligence, Cybersecurity and Cyber Defence

The History and Future of American Intelligence

Understanding Cyber Conflict

Cyber Reconnaissance, Surveillance and Defense

A Multidisciplinary Approach

"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." —Ron Gula, founder and CTO, Tenable Network Security, from the Foreword "Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way." —Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." —Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy." —Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes—resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source tools—including Sguil, Argus, and Ethereal—to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance. Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

“We are dropping cyber bombs. We have never done that before.”—U.S. Defense Department official A new era of war fighting is emerging for the U.S. military. Hi-tech weapons have given way to hi tech in a number of instances recently: A computer virus is unleashed that destroys centrifuges in Iran, slowing that country’s attempt to build a nuclear weapon. ISIS, which has made the internet the backbone of its terror operations, finds its network-based command and control systems are overwhelmed in a cyber attack. A number of North Korean ballistic missiles fail on launch, reportedly because their systems were compromised by a cyber campaign. Offensive cyber operations like these have become important components of U.S. defense strategy and their role will grow larger. But just what offensive cyber weapons are and how they could be used remains clouded by secrecy. This new volume by Amy Zegart and Herb Lin is a groundbreaking discussion and exploration of cyber weapons with a focus on their strategic dimensions. It brings together many of the leading specialists in the field to provide new and incisive analysis of what former CIA director Michael Hayden has called “digital combat power” and how the United States should incorporate that power into its national security strategy.

Cyber Reconnaissance, Surveillance and DefenseSyngress Press
ECCWS 2020 20th European Conference on Cyber Warfare and Security
Ethical Hacking and Penetration Testing Made Easy
Cyber Strategy
Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges
Intelligence Community Legal Reference Book
North Korea's Cyber Operations
Espionage, Strategy, and Politics in the Digital Domain