Cyber Threats From China Russia And Iran Protecting American Critical Infrastructure

This is likewise one of the factors by obtaining the soft documents of this **Cyber Threats From China Russia And Iran Protecting American Critical Infrastructure** by online. You might not require more become old to spend to go to the books inauguration as well as search for them. In some cases, you likewise attain not discover the pronouncement Cyber Threats From China Russia And Iran Protecting American Critical Infrastructure that you are looking for. It will unconditionally squander the time.

However below, when you visit this web page, it will be fittingly completely simple to acquire as competently as download lead Cyber Threats From China Russia And Iran Protecting American Critical Infrastructure

It will not allow many times as we explain before. You can complete it while pretend something else at home and even in your workplace. correspondingly easy! So, are you question? Just exercise just what we present below as capably as review **Cyber Threats From China Russia And Iran Protecting American Critical Infrastructure** what you gone to read!

Foreign Cyber Threats to the United States Committee on Armed Services United State 2019-10-10 Every American should be alarmed by Russia's attacks on our Nation. There is no national security interest more vital to the United States of America than the ability to hold free and fair elections without foreign interference. That is why Congress must set partisanship aside, follow the facts, and work together to devise comprehensive solutions to deter, defend against and, when necessary, respond to foreign cyber attacks. As we do, we must recognize that the recent Russian attacks are one part of a much bigger cyber problem. Russian cyber attacks have targeted the White House, the Joint Staff, the State Department, our critical infrastructure. Chinese cyber attacks have reportedly targeted NASA, the Departments of State and Commerce, congressional offices, military labs, the Naval War College, and United States businesses, including major defense contractors. Most recently, China compromised over 20 million background investigations at the Office of Personnel Management. Iran has used cyber tools in recent years to attack the United States Navy, United States partners in the Middle East, major financial institutions, and a dam just 25 miles north of New York City. Of course, North Korea was responsible for the massive cyber attack on Sony Pictures in 2014. What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk.
The Russia-China Axis Douglas E. Schoen 2014-09-09 The United States is a nation in crisis. While Washington’s ability to address our most pressing challenges has been rendered nearly impotent by ongoing partisan warfare, we face an array of foreign-policy crises for which we seem increasingly unprepared. Among these, none is more formidable than the unprecedented partnership developing between Russia and China, suspicious neighbors for centuries and fellow Communist antagonists during the Cold War. The two longtime foes have drawn increasingly close together because of a confluence of geostrategic, political, and economic interests—all of which have a common theme of diminishing, subverting, or displacing American power. While America’s influence around the world recedes—in its military and diplomatic power, in its political leverage, in its economic might, and, perhaps most dangerously, in the power and appeal of its ideas—Russia and China have seen their influence increase. From their support for rogue regimes such as those in Iran, North Korea, and Syria to their military and nuclear buildups to their aggressive use of cyber warfare and intelligence theft, Moscow and Beijing are playing the game for keeps. Meanwhile America, pledged to “leading from behind,” no longer does much leading at all. In The Russia-China Axis, Douglas E. Schoen and Melik Kaylan systematically chronicle the growing threat from the Russian-Chinese Axis, and they argue that only a rebirth of American global leadership can counter the corrosive impact of this antidemocratic alliance, which may soon threaten the peace and security of the world.
Return to Winter Douglas E. Schoen 2015-12-01 The United States is a nation in crisis. While Washington’s ability to address our most pressing challenges has been rendered nearly impotent by ongoing partisan warfare, we face an array of foreign-policy crises for which we seem increasingly unprepared. Among these, none is more formidable than the unprecedented partnership developing between Russia and China, suspicious neighbors for centuries and fellow Communist antagonists during the Cold War. The two longtime foes have drawn increasingly close together because of a confluence of geostrategic, political, and economic interests—all of which have a common theme of diminishing, subverting, or displacing American power. While America’s influence around the world recedes—in its military and diplomatic power, in its political leverage, in its economic might, and, perhaps most dangerously, in the power and appeal of its ideas—Russia and China have seen their influence increase. From their support for rogue regimes such as those in Iran, North Korea, and Syria to their military and nuclear buildups to their aggressive use of cyber warfare and intelligence theft, Moscow and Beijing are playing the game for keeps. Meanwhile America, pledged to “leading from behind,” no longer does much leading at all. In Return to Winter, Douglas E. Schoen and Melik Kaylan systematically chronicle the growing threat from the Russian-Chinese Axis, and they argue that only a rebirth of American global leadership can counter the corrosive impact of this antidemocratic alliance, which may soon threaten the peace and security of the world.
The Hacked World Order Adam Segal 2016-02-23 In this updated edition of The Hacked World Order, cybersecurity expert Adam Segal offers unmatched insight into the new, opaque global conflict that is transforming geopolitics. For more than three hundred years, the world wrestled with conflicts between nation-states, which wielded military force, financial pressure, and diplomatic persuasion to create "world order." But in 2012, the involvement of the US and Israeli governments in Operation "Olympic Games," a mission aimed at disrupting the Iranian nuclear program through cyberattacks, was revealed; Russia and China conducted massive cyber-espionage operations; and the world split over the governance of the Internet. Cyberspace became a battlefield. Cyber warfare demands that the rules of engagement be completely reworked and all the old niceties of diplomacy be recast. Many of the critical resources of statecraft are now in the hands of the private sector, giant technology companies in particular. In this new world order, Segal reveals, power has been well and truly hacked.
Dawn of the Code War John P. Carlin 2018-10-16 The inside story of how America's enemies launched a cyber war against us-and how we've learned to fight back With each passing year, the internet-linked attacks on America's interests have grown in both frequency and severity. Overmatched by our military, countries like North Korea, China, Iran, and Russia have found us vulnerable in cyberspace. The "Code War" is upon us. In this dramatic book, former Assistant Attorney General John P. Carlin takes readers to the front lines of a global but little-understood fight as the Justice Department and the FBI chases down hackers, online terrorist recruiters, and spies. Today, as our entire economy goes digital, from banking to manufacturing to transportation, the potential targets for our enemies multiply. This firsthand account is both a remarkable untold story and a warning of dangers yet to come.
The Future of Global Competition Robert Hinck 2021-12-01 With today’s social and geopolitical order in

significant flux this project offers vital insight into the future global order by comparatively charting national media perceptions regarding the future of global competition, through the lens of Ontological Security (OS). The authors employ a mixed-method approach to analyze 620 news articles from 47 Russian, Chinese, Venezuelan, and Iranian news sources over a five-year period (2014-2019), quantitatively comparing the drivers of their visions while providing in-depth qualitative case studies for each nation. Not only do these narratives reveal how these four nations understand the current global order, but also point to their (in)flexibility and agentic capacity for reflection in adapting, even shaping the future order, and their identity-roles within it, around an economic and diplomatic battleground. The authors argue these narratives create trajectories with inertial effects grounded in their OS needs, providing enduring insights into their behavior and interests moving into the future. The Future of Global Coopetition will help readers understand how influential nations typical aligned in opposition to the US, envision the drivers of global competition and the make-up of the future international system. Those engaged in the study of media, global politics, international relations, and communication will find this book to be a critical source.

Cyber Threats from China, Russia, and Iran United States. Congress 2017-12-12 Cyber threats from China, Russia, and Iran : protecting American critical infrastructure : hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, One Hundred Thirteenth Congress, first session, March 20, 2013.

Industry Perspectives on the President's Cybersecurity Information-Sharing Proposal Infrastru Subcommittee on Cybersecurity 2015-07-03 For years, the private sector has been on the front line battling devastating cyber attacks from criminals, activists in nation-states such as Iran, China, Russia, and North Korea. Any cyber threat-sharing legislation produced by Congress should enhance existing capabilities and relationships while establishing procedures to safeguard personal privacy. The cyber breach of health insurance giant Anthem exposed the personal information of up to 80 million Americans, approximately 1 in every 4 Americans, demonstrating that the quantity and sophistication of these attacks is only increasing. The director of national intelligence, James Clapper, underscored this fact, stating that cyber attacks against the U.S. are increasing in frequency, scale, sophistication, and severity of impact and that the methods of attack and the systems targeted and the victims are also expanding in diversity and intensity on a daily basis.

Annual Threat Assessment Director of Nat'l Intelligence 2021-04 "The American people should know as much as possible about the threats facing our nation and what their intelligence agencies are doing to protect them." -Avril Haines, Director of National Intelligence (2021) Annual Threat Assessment of the US Intelligence Community (2021) is an annual report of worldwide threats to the national security of the United States compiled by the US Intelligence Community. It warns of the many perils facing the US, including China's increasing power, the geopolitical risks of Russia, Iran and North Korea, the long-term economic fallout of COVID-19, and global as well as domestic terrorism. This brief report with its short-term threat assessment is a good companion guide to Global Trends 2040-A More Contested World a 2021 report by the National Intelligence Council, which describes specifically long-term global challenges (also available from Cosimo Reports). Students of national security, policymakers, journalists, and anyone interested in US security will find this report essential reading.

Defeating Communism One More Time Mark A. RUSSO CISSP-ISSAP 2019-09-22 AN ESSAY AND A SOLUTIONWhile the Trump Administration has recruited some of the best (and controversial) minds in fighting global terrorism, it has yet to identify and recruit experts with the credentials to defeat threats to the US and its allies in cyberspace. The Chinese cyber threat is the #1 menace in the domain of cyberspace as well as Russia, Iran, and North Korea. While the US was historically focused on the former Soviet Union, i.e., Russia, and more recently in the physical world, the threat of radical jihadist terrorism, the Chinese have grown economically, technologically, militarily, and politically to pose the gravest threat to US cyber interests. The solution to defeating Chinese cyber operations may be found in the leveraging the Administration's counter-terror expertise and applying principles from seasoned experts to thwart and defeat government-sponsored Chinese hackers. The solution will more be found in active use of "soft cyber power" (SCP), that is primarily information dominance focused, AND "hard-cyber power" (HCP), which will be the more comprehensive solution to defeating Chinese supremacy in cyberspace.Soft Military-Information Dominance in the "Age of China"

The Perfect Weapon David E. Sanger 2018-06-19 NOW AN HBO® DOCUMENTARY FROM AWARD-WINNING DIRECTOR JOHN MAGGIO • “An important—and deeply sobering—new book about cyberwarfare” (Nicholas Kristof, New York Times), now updated with a new chapter. The Perfect Weapon is the startling inside story of how the rise of cyberweapons transformed geopolitics like nothing since the invention of the atomic bomb. Cheap to acquire, easy to deny, and usable for a variety of malicious purposes, cyber is now the weapon of choice for democracies, dictators, and terrorists. Two presidents—Bush and Obama—drew first blood with Operation Olympic Games, which used malicious code to blow up Iran’s nuclear centrifuges, and yet America proved remarkably unprepared when its own weapons were stolen from its arsenal and, during President Trump’s first year, turned back on the United States and its allies. And if Obama would begin his presidency by helping to launch the new era of cyberwar, he would end it struggling unsuccessfully to defend against Russia’s broad attack on the 2016 US election. Moving from the White House Situation Room to the dens of Chinese government hackers to the boardrooms of Silicon Valley, New York Times national security correspondent David Sanger reveals a world coming face-to-face with the perils of technological revolution, where everyone is a target. “Timely and bracing . . . With the deep knowledge and bright clarity that have long characterized his work, Sanger recounts the cunning and dangerous development of cyberspace into the global battlefield of the twenty-first century.”—Washington Post

Confronting an Axis of Cyber?: China, Iran, North Korea, Russia in Cyberspace Fabio Rugge 2018 The first Report of the ISPI Center on Cybersecurity focuses on the behaviour of these "usual suspects," investigates the security risks implicit in the mounting international confrontation in cyberspace, and highlights the current irreconcilable political cleavage between these four countries and the West.

Cyber Threats from China, Russia, and Iran United States. Congress. House. Committee on Homeland Security. Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies 2013

Artificial Intelligence, China, Russia, and the Global Order Air University Air University Press 2019-10-19 Given the wide-ranging implications for global competition, domestic political systems and daily life, US policymakers must prepare for the impacts of new artificial intelligence (AI)-related technologies. Anticipating AI's impacts on the global order requires US policy makers' awareness of certain key aspects of the AI-related technologies--and how those technologies will interact with the rapidly changing global system of human societies. One area that has received little in-depth examination to date is how AI-related technologies could affect countries' domestic political systems--whether authoritarian, liberal democratic, or a hybrid of the two--and how they might impact global competition between different regimes. This work highlights several key areas where AI-related technologies have clear implications for globally integrated strategic planning and requirements.

Triple-Axis Ariane Tabatabai 2018-07-30 The most significant challenge to the post-Cold War international order is the growing power of ambitious states opposed to the West. Iran, Russia and China each view the global structure through the prism of historical experience. Rejecting the universality of Western liberal values, these states and their governments each consider the relative decline of Western economic hegemony as an opportunity. Yet cooperation between them remains fragmentary. The end of Western sanctions and the Iranian nuclear deal; the Syrian conflict; new institutions in Central and East Asia: in all these

areas and beyond, the potential for unity or divergence is striking. In this new and comprehensive study, Ariane Tabatabai and Dina Esfandiary address the substance of this `triple axis' in the realms of energy, trade, and military security. In particular they scrutinise Iran-Russia and the often overlooked field of Iran-China relations. Their argument - that interactions between the three will shape the world stage for decades to come - will be of interest to anyone looking to understand the contemporary international security puzzle.

The United States, Russia, and China Paul J. Bolt 2008 Neatly embodying the international cooperation it describes, this book, whose authors are from the United States, Russia, and China, demonstrates how three key powers can cooperate in managing and responding to global security threats.

2017 U.S. Intelligence Community Worldwide Threat Assessment - Coats Testimony Dan R. Coats 2017-05-12 Director of National Intelligence Daniel R. Coats presented the 2017 annual U.S. intelligence community worldwide threat assessment in Congressional testimony on May 11, 2017. In the published report, Coats provides a thorough review of the status of possible threats from a wide variety of nations and terror groups. In addition to the 2017 assessment, this compilation includes the 2016 assessment for comparison and historical reference, plus important additional material, including the Report of the Select Committee on Intelligence, United States Senate, Covering the Period January 6, 2015 to January 2, 2017. Topics covered include: GLOBAL THREATS - Cyber Threat * Emerging and Disruptive Technologies * Terrorism * Weapons of Mass Destruction and Proliferation * Space and Counterspace * Counterintelligence * Transnational Organized Crime * Economics and Natural Resources * Human Security REGIONAL THREATS - East Asia * China * North Korea Southeast Asia * Russia and Eurasia * Russia * Ukraine, Moldova, and Belarus * The Caucasus and Central Asia * Europe * Key Partners * Turkey * Middle East and North Africa * Syria * Iraq * Iran * Yemen * South Asia * Afghanistan * Pakistan * India-Pakistan * Sub-Saharan Africa * South Sudan * Sudan * Nigeria * Sahel * Somalia * Ethiopia * Democratic Republic of the Congo * Western Hemisphere * Mexico * Central America * Colombia * Cuba * Venezuela Coats reported: Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years. Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the US and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. These threats are amplified by our ongoing delegation of decisionmaking, sensing, and authentication roles to potentially vulnerable automated systems. This delegation increases the likely physical, economic, and psychological consequences of cyber attack and exploitation events when they do occur. Many countries view cyber capabilities as a viable tool for projecting their influence and will continue developing cyber capabilities. Some adversaries also remain undeterred from conducting reconnaissance, espionage, influence, and even attacks in cyberspace.

China-Russia Security Relations : Strategic Parallelism Without Partnership Or Passion? Richard Weitz 2008

Cyber Capabilities and National Power 2021 This report sets out a new methodology for assessing cyber power, and then applies it to 15 states: Four members of the Five Eyes intelligence alliance - the United States, the United Kingdom, Canada and Australia ; Three cyber-capable allies of the Five Eyes states - France, Israel and Japan ; Four countries viewed by the Five Eyes and their allies as cyber threats - China, Russia, Iran and North Korea ; Four states at earlier stages in their cyber-power development - India, Indonesia, Malaysia and Vietnam. The methodology is broad and principally qualitative, assessing each state's capabilities in seven different categories. The cyber ecosystem of each state is analysed, including how it intersects with international security, economic competition and military affairs. On that basis the 15 states are divided into three tiers: Tier One is for states with world-leading strengths across all the categories in the methodology, Tier Two is for those with world-leading strengths in some of the categories, and Tier Three is for those with strengths or potential strengths in some of the categories but signi cant weaknesses in others. The conclusion is that only one state currently merits inclusion in Tier One. Seven are placed in Tier Two, and seven in Tier Three.

U.S. and Iranian Strategic Competition D. Brandon Fite 2011 This report shows that China and Russia stand at the pivot of US-Iranian competition with China leaning toward Iran, and Russia leaning, more gradually, to the West. As major world powers and permanent members of the UN Security Council, both nations are essential to either inhibiting or shielding Iran's nuclear and regional ambitions. Neither China nor Russia is fully committed to either competitor, and both are engaged in a complex balancing act: leveraging support to advance their own positions while at the same minimizing the diplomatic costs of double-dealing. To secure Chinese and Russian support, the US and Iran stress the value of their relationship and the costs of partnership with the other. The struggle to capture Chinese support centers on energy security but is framed as a contest of worldviews. The US works to integrate China into the present international order, while Iran rejects the status quo and urges China, as a fellow non-Western power, to create a new system apart from the West. Competition plays out over issues of proliferation and sanctions, trade and energy investments, and arms sales. Importantly, Iran seeks to win Chinese support by billing itself as a secure and dedicated source of energy resources for a century of Chinese growth. China has been able to maintain positive if somewhat strained relations with both the US and Iran by selectively supporting each side. As both a supporter and spoiler, China exploits it dual-role as Iranian benefactor and permanent member of the Security Council, and serves as a de facto gatekeeper to meaningful international sanctions of Iranian nuclear ambitions. China is willing to use US competition with Iran as an opportunity to grow its influence and test the boundaries of the US-led international order. Its moves are calculated to reap the benefits of US-Iranian conflict while deemphasizing the costs associated with supporting both sides. Unlike China whose overriding interest in Iran is energy security, Russia has a multiplicity of interests, none of which are predominant. As a result, Russia's approach to Iran is both broader and more flexible than the PRC's, and the US and Iran compete for Russian support on an issue-by-issue basis. The primary areas of competition are proliferation and sanctions, trade and energy deals, nuclear technology and infrastructure sales, arms sales, and influence in the Gulf and Middle East. Russia has historically been an important contributor to Iran's nuclear infrastructure and conventional arms capacity, but relations between the two states have been impacted by intensifying Iranian competition with the West and warming Russian relations with the US in the wake of the Obama administration's "reset" policy. Russia has begun to cooperate with the US in meaningful ways, but Moscow's move away from Tehran should not be interpreted as a wholesale shift in Russian policy. Russia's strategy to maintain coeval relations with the US and Iran has been to portray itself as an intermediary power. By cooperating on a limited basis with the West while advocating for a softer approach to Iran, Russia reaps the benefits of selective cooperation without incurring the costs of full allegiance. The ties that bind China and Russia to Iran are primarily based on an opportunistic assessment of the costs and benefits of partnership. Leaders in Moscow and Beijing are principally concerned with the security and prosperity of their nations, and they will pursue international relationships from that standpoint. External pressure is not yet significant enough to negate the fruits of cooperation with Tehran. If the US is to be successful in its attempt to isolate Iran by severing these great power connections, it must work to upset their present cost-benefit calculations.

Cyber Threats from China, Russia, and Iran Committee on Homeland Security House of Representatives 2014-01-17 Today's hearing is timely and very relevant. We are examining the cyber threat today that is posed by nation-states, namely China, Russia, and Iran. I focus on the nation-state aspect of this threat because it represents a new battlefield in state relationships and one in which we must prepare accordingly. There have been significant developments in the cyber domain,

highlighted by the fact that the U.S. Government has finally begun to name the nation-states most responsible for cyber attacks against the United States. Tom Donilon, the President's National security adviser, outed China as the place where cyber intrusions are emanating on an unprecedented scale. The annual threat assessment by the United States intelligence community delivered to Congress-Director of National Intelligence, James Clapper, named cyber as the top threat to the United States' National security. This represents a major shift in the threat assessment by the United States intelligence community and makes our work on this committee even more important.

Cyber Mercenaries Tim Maurer 2018-01-18 Cyber Mercenaries explores how and why states use hackers as proxies to project power through cyberspace.

National Security (A Study of Myanmar, Russia, Iran) Ahmad Reza Taheri

Cyber Strategy Brandon Valeriano 2018-04-17 Some pundits claim cyber weaponry is the most important military innovation in decades, a transformative new technology that promises a paralyzing first-strike advantage difficult for opponents to deter. Yet, what is cyber strategy? How do actors use cyber capabilities to achieve a position of advantage against rival states? This book examines the emerging art of cyber strategy and its integration as part of a larger approach to coercion by states in the international system between 2000 and 2014. To this end, the book establishes a theoretical framework in the coercion literature for evaluating the efficacy of cyber operations. Cyber coercion represents the use of manipulation, denial, and punishment strategies in the digital frontier to achieve some strategic end. As a contemporary form of covert action and political warfare, cyber operations rarely produce concessions and tend to achieve only limited, signaling objectives. When cyber operations do produce concessions between rival states, they tend to be part of a larger integrated coercive strategy that combines network intrusions with other traditional forms of statecraft such as military threats, economic sanctions, and diplomacy. The books finds that cyber operations rarely produce concessions in isolation. They are additive instruments that complement traditional statecraft and coercive diplomacy. The book combines an analysis of cyber exchanges between rival states and broader event data on political, military, and economic interactions with case studies on the leading cyber powers: Russia, China, and the United States. The authors investigate cyber strategies in their integrated and isolated contexts, demonstrating that they are useful for maximizing informational asymmetries and disruptions, and thus are important, but limited coercive tools. This empirical foundation allows the authors to explore how leading actors employ cyber strategy and the implications for international relations in the 21st century. While most military plans involving cyber attributes remain highly classified, the authors piece together strategies based on observations of attacks over time and through the policy discussion in unclassified space. The result will be the first broad evaluation of the efficacy of various strategic options in a digital world.

Central Asian Security Roy Allison 2004-05-13 This volume is the first comprehensive scholarly analysis of the strategic reconfiguration of Central Asia as Russia has become more disengaged from the nations in the region and as these nations have developed new relations to the south, east, and west. The international implications are enormous because of the rich energy sources—oil and natural gas—located in the Caspian Sea area. The authors assess a variety of internal security policy challenges confronting these states—for example, the potential for conflict arising from such factors as a mixed ethnic population, resource scarcity, particularly in relation to water management, and an Islamic revival. They also examine the security policy content of relations between the Central Asian states and regional and international powers—specifically the stakes, interests, and policies of Russia, China, Iran, Turkey, and the United States. These internal challenges and the evolution of relations with external powers may result in new cooperative relationships, but they may also lead to destabilizing rivalry and interstate enmity in Central Asia. It is important to identify new patterns of relevance for future security cooperation in the region, but the potential for a new security system or for new institutions to manage security in the region remains uncertain. These issues are explored by a team of prominent specialists from Western Europe, the United States, Russia and China.

The Hacker and the State Ben Buchanan 2020-02-28 “One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from underseas cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent. With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph.

The U.S. Cybersecurity and Intelligence Analysis Challenges John Michael Weaver

Cyber Threat: The Rise of Information Geopolitics in U.S. National Security Chris Bronk 2016-02-01 This book presents a holistic view of the geopolitics of cyberspace that have arisen over the past decade, utilizing recent events to explain the international security dimension of cyber threat and vulnerability, and to document the challenges of controlling information resources and protecting computer systems. • Provides relevant, rigorous information to those in the computer security field while also being accessible to a general audience of policy, international security, and military readers who seek to understand the cyber security issue and how it has evolved • Documents how contemporary society is dependent upon cyberspace for its function, and that the understanding of how it works and how it can be broken is knowledge held by a precious few • Informs both technically savvy readers who build and maintain the infrastructure of cyberspace and the policymakers who develop rules, processes, and laws on how the cyber security problem is managed

Confronting an "Axis of Cyber"? Fabio Rugge 2018-10-24 The new US National Cyber Strategy points to Russia, China, North Korea and Iran as the main international actors responsible for launching malicious cyber and information warfare campaigns against Western interests and democratic processes. Washington made clear its intention of scaling the response to the magnitude of the threat, while actively pursuing the goal of an open, secure and global Internet. The first Report of the ISPI Center on Cybersecurity focuses on the behaviour of these “usual suspects”, investigates the security risks implicit in the mounting international confrontation in cyberspace, and highlights the current irreconcilable political cleavage between these four countries and the West in their respective approaches “in and around” cyberspace.

Emerging Cyber Threats to the United States Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives Subcommittee 2017-05-05 The United States faces evolving cybersecurity threats from nation-states such as China, Russia, North Korea, and Iran, as well as cyber threats from criminal organizations and terrorist groups such as ISIS. These actors continue to develop and build more sophisticated cyber capabilities. These hackers now pose an even greater threat to the U.S. homeland and critical infrastructure. Cybersecurity more than ever is National security. In 2015, the U.S. was the victim of one of the most significant cyber attacks in its history. The breach at the Office of Personnel Management exposed the personal and security clearance information of 21.5 million current and former Government employees. In 2014, North Korea conducted a cyber attack on Sony Pictures that not only destroyed computers, but also was intended to stifle free speech and threaten American ideals. The Obama administration's lack of proportional responses to these cyber attacks has signaled to the world that there are no real consequences for such actions. Without a comprehensive National cybersecurity strategy that establishes deterrence, the future could bring an increasing number of adversaries that are willing to conduct cyber attacks against the United States.

The Power to Coerce David C. Gompert 2016-02-25 Mounting costs, risks, and public misgivings of waging war are raising the importance of U.S. power to coerce (P2C). The best P2C options are financial sanctions, support for nonviolent political opposition to hostile regimes, and offensive cyber operations. The state against which coercion is most difficult and risky is China, which also happens to pose the strongest challenge to U.S. military options in a vital region.

Cyber Threats from China, Russia, and Iran United States. Congress. House. Committee on Homeland Security. Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies 2013

China, Russia, and Twenty-First Century Global Geopolitics Paul J. Bolt 2018-02-15 This book provides a comprehensive analysis of the Chinese-Russian bilateral relationship, grounded in a historical perspective, and discusses the implications of the burgeoning "strategic partnership" between these two major powers for world order and global geopolitics. The volume compares the national worldviews, priorities, and strategic visions for the Chinese and Russian leadership, examining several aspects of the relationship in detail. The energy trade is the most important component of economic ties, although both sides desire to broaden trade andinvestments. In the military realm, Russia sells advanced arms to China, and the two countries engage in regular joint exercises. Diplomatically, these two Eurasian powers take similar approaches to conflicts in Ukraine and Syria, and also cooperate on non-traditional security issues includingpreventing coloured revolutions, cyber management, and terrorism. These issue areas illustrate four themes. Russia and China have common interests that cement their partnership, including security, protecting authoritarian institutions, and re-shaping aspects of the global order. They are keyplayers not only influencing regional issues, but also international norms and institutions. The Sino-Russian partnership presents a potential counterbalance to the United States and democratic nations in shaping the contemporary and emerging geopolitical landscape. Nevertheless, the West is still an important partner for China and Russia. Both seek better relations with the West, but onthe basis of "mutual respect" and "equality". Lastly, Russia and China have frictions in their relationship, and not all of their interests overlap. The Sino-Russian relationship has gained considerable momentum, particularly since 2014 as Moscow turned to Beijing attempting to offset tensions withthe West in the aftermath of Russia's annexation of Crimea and intervention in Ukraine. However, so far, China and Russia describe their relationship as a comprehensive 'strategic partnership', but they are not 'allies'.

Essays in Technology, Security and Strategy Shoshana Bryen 2020 Powerful writings focused on how technology impacts national security decision making and strategy. Volume III covers NATO, Russia, Korea, China, Middle East, Terrorism, Weapons, Technology and more. Learn more than anywhere else about missile defense, hypersonic weapons, drones and cruise missiles and the latest from threats from China, Iran, North Korea and Russia. Understand how the US, its allies and friends (including Israel) are responding to changing military and political challenges. "The third volume of Stephen Bryen's essays on technology and diplomacy is about to appear. You will look far and wide to find anything comparable. Steve was a brilliant officer in Ronald Reagan's Pentagon, and then a wizard at the head of Finmeccanica, the Italian company's American division. The current batch of essays explores the complicated ways in which the post-Cold War world seeks to sort itself into a new paradigm. There is no one better." --Michael Ledeen, Historian, Author and adviser to the Secretary of State "I never fail to gain new insights from reading Dr. Stephen Bryen's books and essays and Volume III of "Essays in Technology, Security and Strategy" is no exception. I highly recommend it to anyone interested or working in international security matters." --The Honorable David Q. Bates, Jr.Assistant to the President and Secretary to the Cabinet for former President George H. W. Bush "These thoughtful essays help illuminate the essential but insufficiently understood nexus between technology and national security strategy. This volume should be of immense interest and value to foreign policy professionals in a rapidly changing world." --Clifford D. May Founder and president, Foundation for Defense of Democracies" As a defense reporter for more than 30 years, I was heavily reliant on the foresight, analysis and unquestionable integrity of Steve and Shoshana Bryen. For decades, these courageous bellwethers of emerging threats sounded political, operational and technical alarms way before the mainstream caught up with them. Whether it was the Pentagon's undue dependence on commercial software; Russian advances in hypersonic technology that threatened end-runs around US missile defenses and stealth platforms; or Israel's willingness to award critical infrastructure projects to the Chinese, the Bryen's never pulled punches in their ultimate interest of safeguarding US national security and interests. Kudos on this third volume of essays, which is well worth the read. " --Barbara Opall-Rome Former Israel Bureau Chief, Defense News and founding executive editor/host of "Strictly Security," i24News "A gem of a collection by the architect of America's export security policy during the Reagan years, brilliant cyber security expert, whose deep understanding of theoretical issues (a doctorate in political science didn't hurt) is equaled only by his business savvy. Each of these essays offers profound insights into the strategic challenges of our time - and they are well written, in an easy and clear style." --Juliana Pilon Senior Fellow at the Alexander Hamilton Institute for the Study of Western Civilization in Clinton, New York

Understanding Cyber Conflict George Perkovich 2017-11 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.

Stretching and Exploiting Thresholds for High-Order War Ben Connable 2016-05-05 Russia, China, and Iran use measures short of war to exploit and stretch U.S. thresholds for war to further their strategic ends. This report describes those measures, how nation-states use them, and why U.S. notions of thresholds might be

outdated.
Three Dangerous Men: Russia, China, Iran and the Rise of Irregular Warfare Seth G. Jones 2021-09-07 How three key figures in Moscow, Beijing, and Tehran built ruthless irregular warfare campaigns that are eroding American power. In Three Dangerous Men, defense expert Seth Jones argues that the US is woefully unprepared for the future of global competition. While America has focused on building fighter jets, missiles, and conventional warfighting capabilities, its three principal rivals—Russia, Iran, and China—have increasingly adopted irregular warfare: cyber attacks, the use of proxy forces, propaganda, espionage, and disinformation to undermine American power. Jones profiles three pioneers of irregular warfare in Moscow, Beijing, and Tehran who adapted American techniques and made huge gains without waging traditional warfare: Russian Chief of Staff Valery Gerasimov; the deceased Iranian Major General Qassem Soleimani; and vice chairman of China's Central Military Commission Zhang Youxia. Each has spent his career studying American power and devised techniques to avoid a conventional or nuclear war with the US. Gerasimov helped oversee a resurgence of Russian irregular warfare, which included attempts to undermine the 2016 and 2020 US presidential elections and the SolarWinds cyber attack. Soleimani was so effective in expanding Iranian power in the Middle East that Washington targeted him for assassination. Zhang Youxia presents the most alarming challenge because China has more power and potential at its disposal. Drawing on interviews with dozens of US military, diplomatic, and intelligence officials, as well as hundreds of documents translated from Russian, Farsi, and Mandarin, Jones shows how America's rivals have bloodied its reputation and seized territory worldwide. Instead of standing up to autocratic regimes, Jones demonstrates that the United States has largely abandoned the kind of information, special operations, intelligence, and economic and diplomatic action that helped win the Cold War. In a powerful conclusion, Jones details the key steps the United States must take to alter how it thinks about—and engages in—competition before it is too late.
This Is How They Tell Me the World Ends Nicole Perlroth 2021-02-18 WINNER OF THE FT & McKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 The instant New York Times bestseller A Financial Times and The Times Book of the Year 'A terrifying exposé' The Times 'Part John le Carré . . . Spellbinding' New Yorker We plug in anything we can to the internet. We can control our entire lives, economy and grid via a remote web control. But over the past decade, as this transformation took place, we never paused to think that we were also creating the world's largest attack surface. And that the same nation that maintains the greatest cyber advantage on earth could also be among its most vulnerable. Filled with spies, hackers, arms dealers and a few unsung heroes, This Is How They Tell Me the World Ends is an astonishing and gripping feat of journalism. Drawing on years of reporting and hundreds of interviews, Nicole Perlroth lifts the curtain on a market in shadow, revealing the urgent threat faced by us all if we cannot bring the global cyber arms race to heel.
China, Europe and International Security Frans-Paul van der Putten 2012-02-01 This book examines the roles played by China and Europe in the domain of international security in the 21st century. Bringing together Chinese and European expertise on the Sino-European Security relationship , this book positions Europe - both the EU and the major national actors - and China in a global security context. It offers not merely an elaboration of the theme of bilateral security relations, but also introduces a wider view on Europe and China as global security actors. The chapters cover four main themes: the perceptions of and actual relations between Europe and China as security actors; relations of China and Europe with third parties such as the US, Russia, and Iran; Europe and China as actors in multilateral security approaches; Europe and China as (potential) security actors in each other's technological domain or region. Given the increasingly prominent roles that both China and Europe play in international security as permanent members of the UN Security Council (in the European case, through the informal and partial representation of the UK and France), through their extensive global economic interests, and their important relations with the USA, this book provides a timely examination of the current state and future developments in the Sino-European relationship. This book will be of much interest to students of international security, Chinese politics, EU studies and IR in general.
Cyber War Committee on Foreign Affairs House of Representatives 2015-12-03 It is no exaggeration to say that we are at the dawn of a new age of warfare. Computers and the Internet have connected people around the world. However, reliance on these technologies has also made us vulnerable to cyber attacks from other countries, terrorists, and criminals. So much so that the Pentagon now counts cyberspace as the fifth domain of warfare alongside land, air, sea, and space. Whether or not an all-out cyber war occurs, it is clear that we are in a state of ongoing cyber conflict. The White House, the State Department, and the Department of Defense have all been hacked, and, of course, the Office of Personnel Management had the sensitive information of more than 21 million Americans compromised. In the private sector, hackers have crashed the computers of Sony executives, seized the personal information of more than 78 million people from the Nation's second largest health insurer, and stolen the credit and debit card information of more than 40 million customers of a major retailer. The magnitude of this theft is staggering, yet it takes companies an average of 205 days to even realize their system has been breached. Across the globe, Estonia found itself at the opposite end of a crippling Russia-backed denial of service attack. A computer worm shut down the air force and navies of France and Great Britain for a time. And an attack by North Korea, coined Dark Seoul, crippled South Korea's banking system. In the coming years, it is likely that Iran will pour more resources into cyber weapons. These have already been used against the U.S. Navy, American banks, a Las Vegas casino, and Saudi Arabia's largest oil producer, all without setting off significant retaliation. Indeed, it has been said that it is exactly the lack of international norms in responding that make cyber weapons so attractive to Russia, China, Iran, and North Korea.