

Battlefield cyber

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Battlefield cyber : how China and Russia are undermining our democracy and national security / Michael G. McLaughlin and William J. Holstein

Auteur(s) : McLaughlin, Michael G. officier

Autre(s) auteur(s) : Holstein, William J.

Publication : Essex (Conn.) Lanham (Md.) : Prometheus books, 2023

Description matérielle : 1 vol. (XIV-285 p.) ; 24 cm

ISBN : 978-1-6338-8901-9
1-63388-901-7

EAN : 9781633889019 rel.

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Notes bibliogr. Index

Note sur le contenu : Introduction: All hands on deck Part I: We are at war. Cyber warfare: The enemy inside the gates Water and oil: Weaponized ransomware, digital proxies, and the threat to critical infrastructure Chinese cyber espionage: The greatest transfer of wealth in history The new oil: Data and China's digital silk road strategy Stoking the flames: How malign influence exacerbates America's political divides and ethnic tensions Software meltdown: The problem with trust Someone else's server: The vulnerabilities of cloud computing Stealing the war: Cyber threats to America's defense supply chain Part II: The response: What must be done. Retreat from globalization: Easing corporate America's addiction to China Social disorder: Reining in social media and big tech Re-architecting security: What the private sector must do Government action: What the public sector must do Collective defense: How the public and private sectors must work together Conclusion: The metaverse, education, and restoring the political "center"

Résumé ou extrait : "The United States is being bombarded with cyber-attacks. From the surge in ransomware groups targeting critical infrastructure to nation states compromising the software supply chain and corporate email servers, malicious cyber activities have reached an all-time high. Russia attracts the most attention, but China is vastly more sophisticated. They have a common interest in

exploiting the openness of the Internet and social media-and our democracy-to erode confidence in our institutions and to exacerbate our societal rifts to prevent us from mounting an effective response. Halting this digital aggression will require Americans to undertake sweeping changes in how we educate, organize and protect ourselves and to ask difficult questions about how vulnerable our largest technology giants are." (éd.)

Sujet - Nom commun : Cyberterrorisme -- États-Unis

Cyberterrorisme -- Politique publique -- États-Unis

Guerre de l'information -- États-Unis

Réseaux d'ordinateurs -- Mesures de sûreté -- États-Unis