1.	Record Nr.	UNINA9910631082803321
	Autore	Stoddart Kristan
	Titolo	Cyberwarfare : Threats to Critical Infrastructure / / by Kristan Stoddart
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Palgrave Macmillan, , 2022
	ISBN	9783030972998 9783030972981
	Edizione	[1st ed. 2022.]
	Descrizione fisica	1 online resource (550 pages)
	Collana	Palgrave Studies in Cybercrime and Cybersecurity, , 2946-2789
	Disciplina	364.168 005.8
	Soggetti	Computer crimes Criminology Security, International Terrorism Political violence Data protection Peace Cybercrime Crime Control and Security International Security Studies Terrorism and Political Violence Data and Information Security Peace and Conflict Studies
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Introduction -- Chapter 1: On Cyberwar: Theorizing cyberwarfare through attacks on critical infrastructure – Reality, potential and debates -- Chapter 2: Cyberwar: Attacking Critical Infrastructure -- Chapter 3: Gaining Access: Attack and defense methods and legacy systems -- Chapter 4 – Hacking the human -- Chapter 5: Non and sub-state actors: Cybercrime, terrorism and hackers -- Conclusion. .
	Sommario/riassunto	“Kristan Stoddart brings together an outstanding treatise of one of the

most important subjects in international security of our times… This book offers innovative insights for scholars interested in the security and strategy of cyberwarfare, as well as those interested in understanding the security dynamics of the modern world more generally.” -Christian Kaunert, Professor of International Security, Dublin City University & University of South Wales. “This book provides an exciting level of insight and detail into one of the most obscure and less explored areas of cyberspace studies. It is very informative and extremely interesting to read and I am certain it will be a necessary resource for students and academics in the field of cyber-related studies, international politics and beyond.” — Vasileios Karagiannopoulos, Reader in Cybercrime and Cybersecurity and Director of the Cybercrime Awareness Clinic, University of Portsmouth, UK. This book provides a detailed examination of the threats and dangers facing the West at the far end of the cybersecurity spectrum. It concentrates on threats to critical infrastructure which includes major public utilities. It focusses on the threats posed by the two most potent adversaries/competitors to the West, Russia and China, whilst considering threats posed by Iran and North Korea. The arguments and themes are empirically driven but are also driven by the need to evolve the nascent debate on cyberwarfare and conceptions of ‘cyberwar’. This book seeks to progress both conceptions and define them more tightly. This accessibly written book speaks to those interested in cybersecurity, international relations and international security, law, criminology, psychology as well as to the technical cybersecurity community, those in industry, governments, policing, law making and law enforcement, and in militaries (particularly NATO members). Kristan Stoddart is Associate Professor in Cyber Threats in the School of Social Sciences at Swansea University, UK, a member of Swansea’s Cyber Threats Research Centre (CYTREC), and Visiting Professor at the University of South Wales. He currently holds a grant looking at EU resilience Against Hybrid Warfare. From 2014-17, he worked on a £1.2 million project which analyzed SCADA systems and the Cyber Security Lifecycle co-funded by Airbus Group and the Welsh government from which this book draws.