# Christopher Whyte and Brian M. Mazanec: Understanding cyber warfare. Politics, Policy and Strategy. Second edition. Routledge, 2023.

Mátyás Kiss*

https://doi.org/10.15170/PJIEL.2024.1.7

In recent years, the number of hostile, interstate cyber operations has significantly increased. While only a few dozen occurred a decade ago, nowadays more than a hundred such actions take place annually, according to reputable international organizations.[1] The ongoing Russian-Ukrainian war now entering its second year, is not only happening in the physical space, but also simultaneously in cyberspace, with the parties constantly attacking each other. As the authors put it in the book: "(…) the information revolution has necessarily (and controversially) changed the way in which future wars will be fought to such a degree that conventional military strategy will never be the same again." The authors are widely recognized as experts in the field. Both are university lecturers, as well as authors and co-authors of numerous works related to cyberspace. In addition, Brian Mazanec is a senior executive in the U.S. government.

The second edition of the book was published in 2023. In comparison to the first edition, which was released in 2018, the authors significantly renewed the chapter that dealt with the overview of some major cyber operations. This chapter has now been supplemented with descriptions of attacks that have occurred since the first edition. The role of the information environment is emphasized more prominently, resulting in a new chapter and numerous minor updates compared to the first edition. The updates presented in the second edition reflect advancements in research and practice in the field of national security. Furthermore, the second edition gives greater prominence to non-state actors. However, the authors emphasize that the manuscript was sent to press following the outbreak of the Russian-Ukrainian armed conflict, therefore it does not—nor

* PhD student, University of Pécs, Faculty of Law.

[1] 'Significant Cyber Incidents' (*Center for Strategic and International Studies*) <www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> accessed 16 March 2024; 'Cyber Operations Tracker' (*Council on Foreign Relations*) <www.cfr.org/cyber-operations/>accessed 16 March 2024.

could it—include the long-term impacts of the conflict on cybersecurity and future cyber operations.
In terms of the structural layout, the book consists of fourteen standalone chapters, followed by a glossary and subject index, totaling over 340 pages. The book contains numerous text boxes, tables and figures that can help deepen the understanding of each topic.

In the first chapter of the book, the authors define the focus of the book. They emphasize that the main focus of it is not cybersecurity, but rather cyber conflicts and the associated historical, empirical, theoretical and political issues. The authors emphasize that cybersecurity extends beyond being solely a technical field. It is necessary to understand the historical context and the international and national environment. They adopt a more general definition, arguing that cybersecurity encompasses all processes, procedures, planning, and actions related to the security of social-technical systems. The authors aim to provide a comprehensive introduction to cyber conflicts, as well as key issues related to warfare in the digital domain. Besides defining additional fundamentals, the authors introduce the subsequent chapters of the book.

The second chapter is titled "the technological foundations of the insecurity in the digital age." In this chapter, readers first gain a comprehensive understanding of the history of the internet's development and the technical structure of computer networks. The chapter introduces techniques for ensuring the security of data transmission between computers, along with various threats to information security system. Additionally, this chapter presents the workings of various forms of malicious software and threats to network security.

The third chapter explores the relationship between cyberspace and international relations. Initially, it discusses how cyberspace began to gain prominence in global politics. The authors explain why cyberspace is important from the perspectives of international security and international relations. They shed light on the primary theories of international relations and demonstrate how they apply within the context of cyberspace. The authors express that liberalism in its various formats might be most useful for the research program on cyberspace and international security. Andrew Moravscik is mentioned, as the authors believe, his form of liberalism is closest to the interactions observed in cyberspace. Followers of liberal theories openly reject the notion that everything is about power politics and emphasize international cooperation. Though theoretically it is undeveloped yet, but the authors believe that states are relatively restrained when it comes to responding to major cyber-attacks speaks to the tenets of modern liberalism in that state behavior might be expected to emerge form configurations of political capacity and interests at both the domestic and interstate level. The neoliberal perspective on world politics also a useful framework for understanding how international cooperation might emerge on cybersecurity and other digital issues. According to the authors, when it comes to cyberspace, realism's

main problem lies in the common critique that its structural variants are overly simplistic. Finally, they mention that as the research program on cyberspace and international security continues to develop, it seems likely that researchers will increasingly turn to constructivism to elaborate on and explain patterns of interaction and political behavior in world politics in the digital age. Constructivism holds that the environment in which political actions takes place in social and that the social setting of internationals can essentially provide states and other actors with their core preferences, which is dramatically different from the perspectives of realism and liberalism.

The fourth, fifth, and sixth chapters are closely connected as they present various manifestations of cyber warfare. The fourth chapter begins by placing the emergence of cyberspace since the 1960s into historical context. The authors initiate this historical journey with a leap of over 100 years, dating back to the outbreak of the First World War. They mention Britain's efforts to decode the entire communication of the central powers. After discussing the Great War, the authors introduce the Enigma project and mention the computer famously created by Alan Turing. They showcase the collaboration between the USA and the United Kingdom after World War II and explain how this relationship guided and shaped the computer revolution in the following decades. The fifth chapter discusses offensive cyber operations from a strategic perspective. It presents two major groups of such operations: attacks against computer networks and operations carried out through the 'exploitation' of the computer systems. The sixth chapter points out that relatively few cyber operations resemble some form of traditional warfare. Cyber tools are highly versatile, multi-purpose instruments through which states and other actions can shape favorable conditions concerning their international affairs.

The seventh chapter provides an empirical overview of the history of cyber conflicts. This chapter, which is rich in detail, outlines the dynamics of conflicts occurring in cyberspace. They present the most significant cyber operations of recent times, starting from the early birds and extending to much more sophisticated operations. The authors pay special attention to countries such as the United States, China and Russia.

The eighth chapter discusses how national experiences related to cybersecurity have shaped various approaches to cyber conflicts. It is noted that in most countries around the world, responding to challenges posted by the digitalization of infrastructure and developing various regulations are still the most problematic issues. The chapter begins by outlining cyber policy efforts and then proceeds to present the experiences of countries at the forefront of the cybersecurity discourse. As for the United States, the authors mention that the history of the United States' effort to confront cyber threats to national security is one of a fragmentation and stuttering coordination between stakeholders both inside and outside of the government. The United Kingdom's experiences with cyber-

space roughly parallel those of other major American allies, like Japan, Germany, or France. The authors also highlight that authoritarian states represent a stark departure from the US in terms of how cybersecurity imperatives have been viewed and how cyber capabilities have been developed. While the experiences of the US have encouraged the national security establishment to think of information security in terms of militarized threats to networks, systems, and critical pieces of content, both China and Russia have for some years now viewed the implications of the information revolution for national security processes in remarkably different way. Specifically, both countries' notion of information security has more clearly embraced the ideas namely that the information revolution has been both about the digitization of infrastructure and fundamental changes in the dynamics of the global informational environment. Thus, information security policy that aims to address issues of both national security and political stability must address ideas as much as it must consider technical security.

The emphasis of the ninth chapter is on the national security aspects of cyber warfare. The authors examine elements of national security vulnerable to various forms of cyberwarfare. The tenth chapter describes conflicts that occur below the threshold of traditional warfare and explores why there is an increased occurrence of such disputes stemming from the effects of the information revolution. Moreover, the chapter discusses conflicts known as 'gray zone' conflicts. The eleventh chapter focuses on non-state actors. This chapter describes how the information revolution has altered the nature of activities by non-state actors, encompassing areas such as social activism and terrorism. At the beginning of the chapter, the authors help us navigate through various definitions, such as hackers, hacktivists, cyber terrorists, or proxies.

The twelfth chapter discusses how constraining norms for offensive cyber operations are developing and offers predictions for how they will develop in the future. The chapter accomplishes this by introducing key concepts regarding norms and international law. It also offers predictions and conclusions based on norm evolution theory for emerging-technology weapons. In the final two chapters, the authors look ahead. They examine how artificial intelligence and other not technologies could change the logic and nature of cyber conflicts.

The book is primarily intended for students interested in cybersecurity, defense policy, or international relations. However, I confidently recommend it to a wide audience, including students, experts, or laypersons. One of the major strengths of the work is its complexity. The authors examine various aspects of cyber warfare in a comprehensive manner, as readers can gain strategic, technical, and historical insights. Overall, the book may be an essential reading for those who are conducting research of cyberspace whether they are students, or experts.