Polish Political Science Yearbook, **vol. 50(2), 2021, pp. 177–179**
DOI: https://doi.org/10.15804/ppsy202123 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Lech Wyszczelski
War Studies Academy (Poland)
ORCID: 0000-0003-2063-4281

On Security in Cyberspace

Book Review: Magdalena Molendowska, Rafał Miernik (Eds.), *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia*, Toruń 2020, pp. 328.

As a scientific topic, security has gained global popularity since the 1970s. In Poland, it happened 20 years later after recognizing "security studies" as a scientific discipline and establishing studies upon it at universities. In result, each year, many research reports on security phenomena are published.

In 2020, Adam Marszałek Publishing House published a book about security edited mainly by scholars from Jan Kochanowski University in Kielce. It was divided in three thematic parts, contributed by seventeen authors. That is why editors' role was crucial. Their task was to arrange received works and adjust to editorial requirements (e.g., a form, methodological unity, general consistency, and others). The editors did it all well. However, one can question their choices to the second and third parts. It is due to the lack of mentioning the criteria used for the selection. Are the papers conference or symposium proceedings; or individual invitations? Eventually, though, it does not impact the book's value since it is dedicated to students of security.

The reviewed piece consists of an introduction and three parts. Why does it not have even a synthetic ending? Or a selective and general bibliography shared for all papers? The editors decided for giving a reference list at the end of each text. The introduction was written by the scientific editors. It is concise (though it feels too concise) but properly marking the work's scope.

Part I "International Area and Cybersecurity" is a result of four authors' effort. Andrzej Żebrowski prepared a long paper "Information Activity as a Danger for International Security Environment". As a substantial paper, it is an excellent introduction to detailed terms within

the semantic field of security and remaining works. Nina Stępnicka, Stanisław Wieteski, and Artur Zimny wrote the second paper. It is a specific elaboration of unmanned air vehicles and threats they may be for people. That piece makes an impression of being thematically distanced from the others, since it touches general instead of individual security-related considerations. However, it is a significant voice, drawing attention to modern air transportation means and threats they can pose to civilians. The third paper was written by Adrian Mitręga – "People's Liberation Army's Activity in Cyberspace". Seemingly, it detaches from general reflections on security, but it includes valuable observations. First of all, the author presents PRC's political leadership's substantial engagement in defining military confrontations in cyberspace – birthmarks of war theater, a global military conflict. The author dedicated a lot of space to Chinese military formations prepared for combat in cyberspace, recognized as strategic battlefield. I wish to digress that Chinese diplomacy's leadership has openly declared that since 2015, the PRC prepares for combat (political, economic, and military) for a superpower position, also in cyberspace. Considering these actions, their weaknesses and strengths, I believe the PRC has more of the latter. Also, it tries to draw a line between "information war" and "computer war". Basic threats within these areas are cybercrimes, hacking, online propaganda, and gaps in military cybersecurity systems (Borkowski, 2015, p. 51). Scholars also highlight a possible recognition of participating in electronic combat as spying. There is also reflection about conducting military operations using electronic combat elements. Li Degin, the Deputy Dean of the Faculty of Strategy and War Activity Theory at the War Studies Academy, is a proponent of such a solution (Borkowski, 2015, p. 52). Theorists prove that cyberattacks combined with a possibility to neutralize American satellites and command centers are a special weapon that can hinder American military operations in the Western Pacific. Let us not forget that the US and the PRC pioneer creating spy software for ICT networks. Currently, analysts of the US and the PRC focus on economic intelligence. It is possible that it will be used for military purposes, probably already done by Israel and some Arab states. The last piece in the discussed part is "CIMIC in Cyberspace" of Paweł Chabielski. The shortcut accounts for the assessment of civil-military cooperation in cyberspace. It is strongly recommended to read the paper. The first part of the reviewed book is definitely the best one.

The following ones are much more specific. Their authors are young academic employees, PhD candidates, and some independent researchers. Their works sometimes are based on expert knowledge. That is why I consider them valuable.

The second part „State Security in Cyberspace" is the most extensive in terms of volume. it includes works of eight authors. Jan Zych wrote "Security in Online Environment"; Paweł Górski – "Cyberspace Security in the XXIst Century – A Reader"; Jolanta Grubicka – "The World in the Web – New Quality of Threats for the State"; Piotr Zalewski – "From Netiquette to CSIR's. Origins and Development of Legal and Organizational Regulations for the Common National System of Cybersecurity"; Rafał Kołodziejczyk – "The Republic of Poland's Security in Cyberspace"; Martyna Ostrowska – Intelligent Transportation Systems (ITS) and

Traffic Security improvements"; Renata Gruszczyńska – "Critical Infrastructure – Technologies and Systems Used by the Municipal Police in Kielce"; and Marcin Walczak – "Cybercrime – A Definition, Forms, and Their Socio-Economic Consequences for the Economy". The titles themselves reflect that the authors usually ponder on specific issues. That is why they should be recognized as introductory pieces. However, it does not mean that studies like these should be postponed but addressed to a narrow group of experts. Reading them is strongly recommended.

The last part is entitled „Personal Security in Cyberspace", and contributed by five authors, including Magdalena Molendowska – the author of paper „Security in the Web – Selected Problems"; Rafał Miernik – „Disinformation and fake news on the Internet as Threats for Security in the European Union"; Katarzyna Rzadkowska – „Deepfake as a Cybernetic Threat"; Marcin Banaszek – „Mobile and Online Bank Services Security". Anna Ptaszek ends the book with the paper „Phonoholism Influence at Social Security". Just like the previous one, this part also includes introductory papers written mainly by authors making their first steps in academic careers or experts with very specific expertise. Is that a disadvantage? I do not think so, since the right of young scholars to publish should be respected, with a chance of them publishing seminal works in the future. Moreover, focused studies are necessary for broader theoretical reflection. Thus, interested parties will certainly benefit from reading the reviewed part.

All the presented works were prepared following the editorial and Ministerial standards allowing to include them for parametrization. They have introductions, endings, and meet other Ministerial criteria. References were arranged appropriately, and presented as lists at the end of each paper. However, the latter would benefit from more detailed structures, for example, indicating legal acts. The book was reviewed by prof. Henryk Wyrobek.

Considering the presented reflections, I find the work valuable, as it introduces order to security studies and marks research agenda for further investigations.

Technical edition also deserves attention. The publisher – Adam Marszałek Publishing House – contributed to editing, publishing, and promoting the book. This review serves to encourage readers to familiarize with the work. That, in turn, serves the purpose of broadening knowledge about cyberspace and cybersecurity, both critical in contemporary times.

References:

Borkowski, K. (2015). Koncepcje cyberbezpieczeństwa *w ujęciu Chińskiej Republiki Ludowej – wybrane aspekty*. *Przegląd Bezpieczeństwa Wewnętrznego, 15*(7).