REVIEW DOI 10.52781/cmm.a051

REVIEW: The fifth domain: defending our country, our companies and ourselves in the age of cyber threats.

CLARKE, Richard A.; KNAKE, Robert K. **The fifth domain**: defending our country, our companies and ourselves in the age of cyber threats. [S. l.]: Penguin Press, 2020. ISBN - 978- 0525561989.

Abstract: The book faces an essential contemporary issue: the definition of the limits of action, protection and use of cyberspace as a fifth operational domain, as well as in the measures to be taken to make this environment more secure. Using the term adopted by the US Department of Defense, the authors use practical experience to indicate an agenda that aims to create means to improve the defense of areas such as state security, economics, democracy and privacy.

Keywords: Cyber Threats. Cyberspace. Cybersecurity. Defense.

Resumen: El libro trae una cuestión contemporánea esencial: la definición de los límites de acción, protección y uso del ciberespacio como un quinto dominio operativo, así como las medidas a se adoptar para hacer que este ambiente sea más seguro. Utilizando el término adoptado por el Departamento de Defensa de los Estados Unidos, los autores utilizan la experiencia práctica para indicar una agenda que busca la creación de medios para mejorar la defensa de áreas como la seguridad del Estado, la economía, la democracia y la privacidad.

Palabras Clave: Ciberamenazas Ciberespacio. Ciberseguridad. Defensa.

Rafael Gonçalves Mota
Universidade de Fortaleza.
Faculdade Ari de Sá.
Tribunal de Justiça do Estado do Ceará.
Fortaleza, CE, Brasil.
rafaelgmota@yahoo.com.br

Received: 23 april 2021
Approved: 28 april 2021

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

The book faces an essential contemporary issue: the definition of the limits of action, protection and use of cyberspace as a fifth operational domain, as well as in the measures to be taken to make this environment more secure. Using the term adopted by the US Department of Defense, the authors use practical experience to indicate an agenda that aims to create means to improve the defense of areas such as state security, economics, democracy and privacy.

The work is fundamental not only for those who study and work with cyber security, but for all those responsible for thinking about issues related to national sovereignty, high strategy and national defense policies. Understanding the scope of the concrete threats that exist in cyberspace, especially in view of the immense speed at which the cyber scenario operates, is essential to guide decision makers in the near future.

The basic perspective of the book holds that the panorama of cyberspace is very different from what it was years ago. According to the authors, the main advantage is that the current technologies allow the reduction of the risks represented by offensive actions of a cybernetic nature. That is, as the development of new technologies holds the potential to create new threats, it also provides National States with new and efficient virtual tools to defend their interests and rights.

Initially, the authors point out that cyberspace has a differentiating characteristic from other operational domains (sea, land, air and space), since it is the only one created by man. This fact, by itself, already makes the virtual environment have different characterizing elements, being necessary to adapt and understand the nature of such threats.

In diagnosing risks, not only aggressive actions taken by state and non-state agents should be considered. Defects, flaws and imperfections in nationally developed software and systems - intentional or not - open a gap for malicious activities to occur more easily and potentially more damaging. With that, Clarke and Knake signal that the creation of a cybersecurity policy must take into account such variables.

Still addressing the potential vulnerabilities arising from the characteristics of cyberspace, the authors comment on the decision of the US government to expand the participation of the private sector in the provision of cyber means, especially physical ones. In 2015, the primary internet servers, hitherto managed through a contract with the Department of Commerce, were transferred to private management.

Given this, there is a sharing of responsibility between the public and private sectors, moving beyond the use of means such as "public-private partnerships" and establishing clear spheres of performance sharing. Although the state field is directly responsible for areas such as military action, cyber-criminal investigation and intelligence collection, data protection and private cyber networks are not state responsibility, and there may only be government collaboration in extreme situations or when private action fail.

Recognizing the impossibility for the State to guarantee, by its own and direct means, the security of cyberspace, as well as the impropriety of the private initiative to safeguard the cyber environment, the authors indicate that there is no easy way or decision. The most certain thing would be to find the least bad solution, not necessarily the best one, since none is completely effective or fully adequate.

Since the Barack Obama administration, the United States has devoted itself to building a strategic cybersecurity policy, aiming to endow not only state agents, but also private entities, with a more concrete and effective degree of protection to guarantee action. in cyberspace. An example of this is the creation of the National Strategy for Trusted Identities in Cyberspace (NSTIC). The idea is to provide the virtual environment with safer means of identification, and, consequently, the attribution of the acts performed there.

One of the problems identified by the authors in dealing with the cyber issue is a greater difficulty in imposing a unified security culture in the private environment since, unlike state entities, individuals and companies have more dispersed actions, within their own dimensions of action.

Regarding the military issue, the authors point out that the Pentagon's objective in relation to an operational domain so peculiar to cyberspace is to seek complete control of the virtual system. This objective is even expressly stated in a document dated 2018, which defines the Department of Defense's cyber strategy.

Continuing in the analysis of military action in cyberspace, the authors raise a central question: can an organization directed to war act to reduce tensions and reduce the likelihood of conflicts? Clarke and Knake say the military contribution is critical to reducing tensions and cyber risks. However, this should occur alongside diplomatic action that creates an architecture of international relations and favors the establishment of an environment with less potential and concrete conflicts.

The direction pointed by the authors for the sphere of international relations is the creation of a cyber space built following the example of the "Schengen Area". When considering the hypothetical situation of an international agreement along these lines, it is possible to build common rules for administration and data protection. In this way, the standardization of control and management rules for cyberspace would produce an even safer environment for companies and companies, which will be able to compete according to common rules.

Advancing the analysis, the authors address the need to build efficient mechanisms for the protection of democracies in the virtual domain. They highlight the growing importance of cyberspace in electoral processes, both due to the communication capacity and the evolution of the virtualization technology of the elections.

The authors also emphasize that the development and improvement of artificial intelligence, notably in the field of machine learning, will undergo a significant increase in the next five years, generating more efficient skills for the promotion of means of defense, except that there has also been an improvement in aggressive acts.

The conclusion of the work is that the strategies, tools and policies of administration and use of cyberspace are already known and the effort must now be channeled by the countries to seize the opportunities and, mainly, to make rational choices to outline the next era of cyberspace.


ECEME