



Cyberspace Implication on National Security in the Context of COVID-19 Pandemic

Rezaiguia Hanane^{1,*}

¹University of Echahid Cheikh Larbi Tebessi, Tebessa (Algeria),

hanane.rezaiguia@univ-tebessa.dz

Received: 19 /07 / 2025

Accepted: 31 /12 / 2025

Published: 11 /06 / 2026

Abstract:

This study aims to analyze and interpret cyberspace in its various dimensions, recognizing it as a recent phenomenon on the international stage that emerged from the technological and informational advancements of the twentieth century. The research seeks to document the significant legal and security efforts made by countries, organizations, and institutions to address potential cyber risks and threats.

One of the key findings is that cyberspace has emerged as a new domain for asymmetric security threats, which are increasingly dangerous and less costly for various actors, particularly in light of the ongoing advancements in technology. This was notably demonstrated during the COVID-19 crisis, which provided an opportunity for a rise in security threats from multiple entities.

Keywords: cybersecurity, cyberspace, threat, COVID-19 pandemic..

*Hanane Rezaiguia.

I. INTRODUCTION

Cyberspace has emerged as a new arena for security threats across various sectors, impacting the information security of these fields. The COVID-19 pandemic, which saw the rapid global spread of the virus, paralyzed activities and forced the world to rely on cyberspace for managing affairs and performing functions, consequently leading to the emergence of unprecedented asymmetric threats.

During the pandemic, there was a significant increase in cyberattacks, raising substantial concerns about digital privacy. This situation poses a threat to national security, particularly as nations use advanced technology across various sectors. The surge in military, security, intellectual, and political information content has created a direct link between digital space security and national security.

This research paper will address various concepts related to cyberspace and attempt to explain its relationship with national security. It will also discuss the most significant security threats, particularly in the context of the COVID-19 pandemic, and subsequently explore the key shortcomings and obstacles to their implementation.

The issue at hand is framed as follows:

How has cyberspace emerged as a new threat to national security for countries?

This research paper is organized into several key sections, including a conceptual framework for the study, an analysis of the impact of cyberspace on national security, and an examination of cyber threats in the context of the COVID-19 pandemic.

1. Conceptual Framework of the Study:

This section will provide definitions of the key concepts related to the cyber domain, as well as the main actors and cyber threats involved.

1.1 Cyber domain related- concepts

1.1.1 Cyberspace

Cyberspace is a realm that has emerged from media connectivity and internet linkage, encompassing many characteristics of social space. It serves as a platform for communication and interaction, facilitates routine activities, allows for the expression of individual identity, showcases the self, and fosters social relationships.

The term “cyberspace” was first introduced in 1982 in the short story “Burning Chrome” by American science fiction author William Gibson, who used it to describe the virtual reality created by computers. The term gained widespread popularity in the 1990s as the use of the internet and network communication media dramatically increased (Ben Amra, 2019, p.687).

It is important to note that cyberspace is under constant attack from spies, thieves, and saboteurs..., who infiltrate computer systems to steal personal data and trade secrets, vandalize websites, disrupt services, deploy malicious systems and viruses, conduct fraudulent transactions, and harass individuals and businesses.

The ease of access and availability of various operations on the internet often at no cost (Dorothy, 2019), has introduced significant security threats in the cyber realm for nations. This shift has transformed the concept of security and its associated threats, expanding them beyond traditional analog and non-analog dangers in the physical world to include virtual threats that have real-world implications.

1.1.2 Cybersecurity

There are various definitions regarding this concept. According to the International Telecommunication Union (ITU), cybersecurity is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. (ITU, 2010).

Cybersecurity presents a new security challenge that necessitates the development of new military concepts by nations and organizations. It is particularly essential to enhance defensive doctrines and offensive strategies to operate effectively in cyberspace, as this domain is a source of uncertainty (Duić et al., 2017, p.4).

1.1.3 Cyberwarfare

Cyberwarfare is defined as a "virtual conflict that is intangible in nature, closely mirroring reality, where the tools of engagement consist of electronic confrontations, technical

software, agents of sabotage, and actions taken through keyboards and programmers' clicks, all within an artificial environment" (Hamden & Majda, 2018, p.20).

The term is commonly used to describe various aspects of defending against and attacking information and computer networks in cyberspace, as well as denying the adversary the ability to perform similar actions. It involves the use of information technology as a tool to target the opponent's critical computer systems (Janet & Laurie, 2004, p.2).

1.1.4 Cyber-attacks

NATO has defined cyber-attacks strategically as those that are more frequent, organized, and costly, resulting in damage to the government and its various sectors. This concept was adopted at the Lisbon Summit in late 2010 (Duić et al., op.cit.).

1.1.5 E-crime

Cybercrime refers to any illegal activity that primarily uses computers as a means for committing offenses and theft (Nikhita & Ugander, 2014, p.1)..

1.1.6 Cyber terrorism

Dorothy E. Denning defines it as the intersection of cyberspace and terrorism, referring to unlawful attacks and threats against computer systems and information networks, aimed at intimidating or coercing governments or their citizens to achieve political or social objectives.

Furthermore, attacks must result in violence against individuals or property, or at the very least, cause sufficient harm to instill fear. For instance, cyber terrorism can target computer systems by tampering with air traffic control systems, potentially leading to aircraft collisions, or by disrupting banks and hindering international financial transactions, global stock exchanges, and economic systems (Dorothy, op.cit.)

1.2 The nature and forms of cyber threats

Cybercrimes manifest in various forms, including denial of service attacks, website intrusions, theft, extortion, and data manipulation. They can involve malicious software such as ransomware and spyware, among others. Cyber warfare has become an unavoidable reality (Clive, 2016, p.26) and depending on the actors involved and their intended targets, four distinct types of threats can be identified (PCM, 2013, p.13):

- Cybercrimes: encompass all malicious activities with criminal intent that occur in the digital realm, including online fraud, identity theft, data or intellectual property theft, and financial theft.

- Cyber espionage: refers to the unauthorized acquisition of confidential or classified information.

- Cyber terrorism: refers to the threat of an attack or an actual attack occurring in the virtual space.

- Cyber warfare: involves activities and operations conducted in the cyber domain to gain an operational advantage for the military.

1.3 Threat actors in cyberspace

Below is a typical classification of threat actors based on their motivations (EUPO, 2020, p.58):

- **Cybercriminals:** these professional offenders are primarily motivated by financial gain and represent the most active group in the threat landscape.

- **Insiders:** current or former employees within targeted organizations, such as employers and contractors, can inadvertently or deliberately cause security incidents, often driven by financial incentives.

- **State-sponsored actors:** these individuals are motivated by political and geopolitical agendas.

- **Hacktivists:** individuals driven by social or political movements, with no ties to governments or private companies.

- **Cyberterrorists:** Individuals motivated by extreme political or religious beliefs and ideologies.

2. The impact of cyberspace on national security

The current century has witnessed a unique revolution in the realm of media and communication technology, to the extent that some experts and specialists consider it the fifth domain of conflict, following land, sea, air, and space.

This is due to the rapid proliferation and advancement of this technology, which has become integral to nearly every aspect of life. This is especially true as most countries and governments have adopted smart government models and transitioned to electronic services, significantly reducing effort, time, and costs.

The speed and flexibility of these infrastructures play a crucial role in meeting demands, making their protection against cyber attacks central to national security. An electronic assault on any of these systems could result in thousands of casualties within just a few minutes.

For instance, a breach in transportation systems such as aviation navigation, maritime operations, and railways could result in collisions. Therefore, establishing an effective electronic defense system that acts as a barrier against cyber-attacks is crucial for the national security of countries (Boukebcha, 2017, p.33).

Cyber threats have become one of the primary challenges that nations must confront in the current era, particularly as reliance on the internet increases. This is especially critical in areas related to national security, such as military networks and financial data.

The discussion regarding the importance of addressing these threats has intensified. In this context, the concept of “cybersecurity” (Mokhtar, 2015, p.5) has emerged as a critical dimension of national security, given the potential damages it can inflict, which may surpass those of traditional security concerns.

The primary objective of cybersecurity is to effectively withstand both recognized and unrecognized threats, as well as to respond to and recover from them. This ensures protection against risks or damages that may arise from the disruption or destruction of information and communication technology, or from the misuse of such technologies.

This necessitates the safeguarding of networks, computers, software, and data from attacks, damage, or unauthorized access. In other words, it primarily involves the protection of information. Given the critical importance of cybersecurity in today's society, many countries have prioritized it, especially in light of the emerging manifestations of cyber warfare among major nations (Ben Merzoug & Al-Kar, 2018, p.37)

Since the events of September 11, 2001, there has been a significant shift in focus towards cyberspace as a new security threat, largely due to international incidents, most notably the use of the internet by Al-Qaeda as a battleground against the United States. In 2007, the role of cyberspace became particularly evident as a new domain for hostile operations during the conflict between Estonia and Russia.

In 2008, during the conflict between Russia and Georgia, the cyber-attack involving the Stuxnet virus on Iran's nuclear program in 2010 marked a significant advancement in the evolution of electronic warfare.

Despite the political role that social media networks played during the Arab up-risings in early 2011, they also marked a significant point in raising international awareness regarding cyber security.

Efforts to exert control have emerged following the rise of protests in some of the most democratic nations, such as the United Kingdom and the United States (Chellouch, 2018, p.193). The recent Russian conflict with Ukraine serves as a prominent example of this, where cyberspace has become a crucial battleground among the various parties involved in the war.

In the lead-up to its military intervention, Russia launched cyberattacks against Ukraine that severely disrupted critical infrastructure and compromised data from various official entities, including the government and the Ministry of Defense. In response, Ukraine, with the support of Western nations, executed similar cyberattacks on Russian sites through the efforts of the hacker group Anonymous.

Although the conflict in all its forms within the digital space is still in its early stages, it is poised to experience an unprecedented diversity in methods of conflict, surveillance, defense, and the nature of the parties involved in the coming years, as the battlefield and warfront increasingly shift to the online realm.

This type of conflict is associated with the realms of electronic warfare and new electronic weapons that parallel, if not surpass, their conventional counterparts in terms of destructive outcomes. These weapons have firmly established themselves in the landscape of both armed and unarmed conflicts. In the information age, conflicts are characterized by their persistence, continuing even after the visible manifestations of armed struggle have ceased.

It represents an environment and context that can either lead to a heated escalation towards war through the mobilization of military forces, or reflect a natural pattern of disputes that fall within the competitive dynamics, which are fundamental characteristics of human society.

Additionally, it may involve the activities of international intelligence agencies or the rivalry among companies operating in the fields of communication and information technology (Gherib, 2018, p.114).

In this context, cyber warfare significantly differs from traditional conflicts, as the outcomes or anticipated results of battles in the digital realm remain shrouded in uncertainty.

For instance, in the context of striving for complete control over the institutions and strategic frameworks of nations through the use of information and communication technology weapons, or by attacking information via electronic media.

This ultimately results in the paralysis of these systems and poses a direct threat to national security by targeting decision-making and defense systems of the state, while also aiming to dominate information databases.

Consequently, there is a potential for a reaction based on the legitimate right to self-defense. Additionally, targeting communications, transportation systems, and public services can harm both lives and property. However, one of the most significant threats in cyberspace is cyber terrorism, which manifests in various forms.

Under the influence of cyberspace, often referred to as cyber power, many nations have been compelled to adopt strategies for their cyber defense and to strengthen their centers of power in a manner akin to traditional defense strategies.

This shift is particularly relevant given the distribution of cyber power among various non-state actors and the emergence of threats that increasingly jeopardize the security and stability of nations, coinciding with the current trend towards asymmetric warfare (Boukebcha, op.cit., p.32).

The increasing military dimensions of cyber power on national security, along with the interconnection of cybersecurity with political, economic, legal, and social domains, have prompted the world to sound the alarm and become more aware of cyber threats than ever before. This has led most countries to prioritize cybersecurity and defense issues in their national security and defense policies.

One of the most widely used protective measures implemented by governments for systems is encryption, along with the enhancement of firewalls to monitor all communications to the system, including emails. The term 'firewall' is relatively common and refers to methods of filtering network access, which assists in determining the services that each user is permitted to access (Steve, 2011, p.6).

It is important to note that there is a significant deficiency in the adoption of effective security strategies to combat cyber threats, which places the national security of many countries at considerable risk.

The rapid and unexpected nature of cyber attacks can devastate the capabilities of numerous nations in a very short time and at minimal cost, especially in the absence of robust counter-strategies. Therefore, it is essential to enhance security mechanisms so that countries can effectively combat these threats and close any vulnerabilities that may exist in cyberspace.

Building on the points raised above, there is a growing awareness within the international community regarding the need to implement security mechanisms to ensure better protection, a topic that will be addressed in the following section.

2.1. Security protection mechanisms

There are two essential mechanisms for achieving optimal security protection, which are as follows (Havlicek, 2012, p.6):

2.1.1 Diversity & robust strategies

Diversity in technology: The variety of technologies, operating systems, and software within infrastructure complicates the task for cyber attackers, as they must navigate this diversity across different systems and applications.

Backup strategies: Implementing contingency plans to thwart cyber attacks is essential; for instance, in the event of a power outage, a backup power supply must be utilized, highlighting the need to prepare for potential attack failures.

Importance of resilience: Establishing a robust infrastructure that can withstand cyber threats is crucial, ensuring that multiple layers of security and backup systems are in place to mitigate risks effectively.

2.1.2 Policies and techniques

The policies and technologies: Among the most crucial policies and technologies that should be implemented to counter cyber threats are the following (Steve, op.cit., p.7):

- Identifying and standardizing best practices on the internet
- Fostering a collaborative environment for developing and implementing information security strategies.
- Encouraging global sharing of intelligence regarding emerging threats and vulnerabilities.
- Using strong passwords
- Implementing firewalls
- Establishing a security policy that employs trained personnel to counter cyber-attacks.
- Auditing login trails and file executions.
- Adopting an intrusion detection system to identify harmful activities.
- Relying on encryption to prevent attacks.

3. Cyber threats during the COVID-19 crisis

During the COVID-19 pandemic, global health systems faced repeated attacks. In January and February of 2020, reports emerged regarding phishing campaigns and malware. On February 13, a Chrome browser extension was utilized (O'Donnell, 2020) that employed fake COVID-19 advertisement videos to drain victims' bank accounts, alongside thousands of related websites that used COVID-19 as bait.

Recent reports indicate that hackers have adapted their malicious advertising campaigns to align with COVID-19. Driven by government support measures aimed at assisting individuals and businesses, there has been a significant rise in identity theft, often by persuading victims to click on seemingly trustworthy links and disclose personal information.

According to the head of the information department at the World Health Organization, security incidents targeting health agencies have increased fivefold compared to the same period in 2019.

For instance, The University Hospital of Brno was forced to shut down due to cyberattacks, and on March 13, the Spanish police issued a warning about a cyberattack aimed at Spanish hospitals. On the same day, the World Health Organization reported attempts to infiltrate its networks through a series of fraudulent emails.

Reports have emerged indicating that attackers have impersonated employees of the World Health Organization to carry out cyberattacks. On March 19, IBM revealed a criminal cyber campaign aimed at distributing emails related to the coronavirus, with messages masquerading as the Director-General of the World Health Organization under the subject line "Treatment for Coronavirus".

On April 9, a similar attack occurred where cybercriminals impersonated President Donald Trump and the White House. In late March, there was a surge in attacks utilizing Trojans. On March 25, Kaspersky warned about the Ginp Android banking trojan, which masqueraded as a 'Coronavirus Finder' app. This app claimed to provide information on COVID-19 cases in the area for a small fee, but instead, it stole the credit card details of its victims.

Kaspersky has revealed a new type of COVID-19 inspired scam that impersonates shipping companies, including FedEx, UPS, and DHL, to install a Trojan horse (EUPO, op.cit., pp.70-73).

Cyberattacks targeting critical sectors and services, such as energy, transportation, education, and healthcare, have become increasingly prevalent. In February 2020, Croatia's largest oil company fell victim to ransomware, while in the United States, a natural gas processing plant faced significant risks from cyber threats. Additionally, in the UK, the Maze ransomware group leaked sensitive data from a medical facility involved in coronavirus research after the organization refused to pay the ransom.

Throughout March and April, incidents persisted in both the United States and Europe, characterized by ransomware attacks targeting government entities and public health departments. Notable examples include an attack on the public health district in Illinois, various

assaults on hospitals, and a specific incident involving a Colorado hospital treating COVID-19 patients.

Additionally, confidential data from the American pharmaceutical company ExecuPharm was exposed on the dark web, along with a wide array of sensitive information about the oil exploration firm Berkine, which was compromised by the Maze ransomware operators.

On March 22, Ambry Genetics, a laboratory based in California, reported an email hacking incident that compromised medical information for nearly 233,000 clients. In France, the IT systems utilized by various local authorities fell victim to ransomware attacks, while in Portugal, the large multinational electric power systems were taken over by ransomware, resulting in encryption of their data and a ransom demand of 9.8 million euros.

The COVID-19 pandemic has been exploited by malicious mobile app developers, as researchers uncovered a ransomware program named CovidLock that masquerades as information about the virus. In April, the German Minister of Health received a ransom note titled 'Attack on German hospitals' demanding a payment of 25 million euros. Additionally, in another incident during the same month of 2020, the website of the Italian National Institute was subjected to a cyber attack (Ibid., pp.73)74).

Numerous countries have adopted digital surveillance systems, which have made them more susceptible to cyberattacks. During the latter half of March, researchers identified a malicious Android application named corona live, and cybercriminals have also managed to recruit several individuals involved in money laundering schemes, particularly as the pandemic has impacted the job market, resulting in many unemployed individuals or those working from home.

An example of this is the 'Vasty Health Care Foundation', which, alongside the evolution of e-commerce and the dark web, saw cybercriminals and opportunists exploit the pandemic by selling counterfeit medical masks and fraudulent treatments on e-commerce platforms and social media.

According to Europol, there has been a significant increase in the number of products claiming to treat the coronavirus since the onset of the pandemic, with scammers demanding upfront payments for these services, resulting in consumers losing money without receiving any goods.

The COVID-19 pandemic has resulted in a significant number of employees working from home, conducting interviews through various chat and video applications such as ZOOM, Slack, Skype, WebEx, Google Meet, and Microsoft Teams. However, several vulnerabilities have been identified within these platforms, highlighted by the sale of half a million Zoom accounts on the dark web on April 13, 2020.

In this context, the U.S. Cybersecurity and Infrastructure Security Agency has reported that two separate attacks targeted as many as 50,000 different users of MS Teams. Cybercriminals claimed to have obtained personal details and secrets about their victims by compromising their computers, subsequently demanding a ransom to prevent the disclosure of sensitive information (Ibid., pp.74-79).

The COVID-19 pandemic has significantly impacted various aspects of our daily lives, particularly affecting the fundamental layers of society. While cybersecurity may seem like an unrelated field, it has gained prominence during this period, as cybercriminals view the unexpected surge in demand for digital services as an opportunity to exploit the current situation, targeting businesses, governments, and individuals.

Cybersecurity has become a crucial societal necessity, particularly in the face of global crises. The rise of cyber threats during the COVID-19 pandemic highlighted this need, as there was a significant reliance on the internet and digital services in hospitals, laboratories, government services, and online education. This shift towards digital transformation, while essential, unfortunately also expanded the potential for cyber attacks (Ibid., p.70).

In light of this, preparedness is crucial for effectively mitigating potential impacts and preventing severe consequences in the event of a cyber attack. Therefore, a strategy is established to ensure an appropriate response to incidents and adequate resilience, which is another essential element in reducing the effects of cyber attacks.

When discussing "cyber resilience," it fundamentally refers to a system's ability to remain intact amidst adverse cyber events. Cyber resilience can be seen as the intersection of information security, business continuity, and organizational flexibility. This resilience

encompasses the capacity to prepare for, withstand, recover from, and adapt to pressures, attacks, or compromises affecting electronic resources.

The concept of resilience also encompasses a societal perspective, which pertains to a community's ability to withstand negative impacts from its environment while continuing to function and provide social well-being for both current and future generations. Additionally, resilience can include information and communication technology systems, entire organizations, and even society as a whole.

Electronic resilience measures can be categorized into two distinct groups: the first encompasses all strategies aimed at ensuring a swift and effective response to cyber incidents and recovery from them, while the second includes those measures and preparations designed to ensure that the system remains operational under adverse conditions, allowing it to function even in deteriorating circumstances.

To ensure the system can operate continuously under adverse conditions, it is essential to incorporate resilience into its design. This principle aligns closely with the concept of security by design. The importance of this resilience will only grow as we move beyond the COVID-19 crisis, which has led to a significant increase in online work and remote learning.

A culture of awareness can aid in identifying and resisting attacks while enabling individuals to take appropriate measures, thereby minimizing the impact on each person. Additionally, a culture of collective resilience will help maintain a baseline of trust in services, products, and public digital infrastructure (Ibid., pp.83-93).

II. Conclusion:

The advancement of technology has created a virtual space reliant on electronic devices, posing a genuine and tangible threat to national security. The cyber domain has emerged as the fifth theater of conflict, alongside land, sea, air, and outer space, making cybersecurity one of the most critical dimensions of national security.

This situation has prompted countries to adopt cyber defense strategies and policies that are somewhat capable of addressing various potential threats, thereby mitigating the increasing security risks. Collaboration is a crucial step in this context to alleviate cybersecurity risks, given that it is impossible to completely eliminate these threats.

The COVID-19 crisis posed a significant challenge to national security, particularly due to the heavy reliance on the internet and virtual platforms. This situation has led to an increase in cyberattacks across various sectors, whether for financial gain or other purposes such as espionage and the breach of sensitive data related to the pandemic, as evidenced by the incidents involving American research laboratories mentioned earlier.

Recommendations:

In conclusion, this study highlights the need for greater attention from countries, organizations, and various stakeholders in the cyber domain to foster collaboration aimed at addressing the increasing cyber threats.

III. Referrals and references:

Journal article:

1. Belkacem Amine Ben Amra (2019), *Approaches to the Restriction of Cyberspace: John Rawls's Theory of Justice as a Model*, Al-Nassiriya Journal of Social and Historical Studies, Volume 10, Issue 2, December 2019.
2. Ben MarzougAntar& Al-Kar Mohammad (2018), *Electronic Methods for Security Policy*, Journal of Social Humanities, Issue 38.
3. Boukhebcha Mohammed (2017), *Cyber Defense*, Join the Army, Issue 651.
4. Gharib Hakim (2018), *Global Cyber Terrorism and International Adjustment: The New Become and Adaptation Methods*, Algerian Journal of Political Science, Volume 5, Issue 2.
5. Hamden Mohammed Tayeb&KhanchMajda (2018), *Cyberwars Emerging from State-Based Instances*, Journal of Legal and Political Studies, N°.7.
6. Janet J. Pritchard and Laurie E. MacDonald (2004), *Cyberterrorism: A Study of the Extent of Coverage in Computer Security Textbooks*, Journal of Information Technology Education, Volume 3, 2004.DOI:[10.28945/302](https://doi.org/10.28945/302)
7. Mohammad Mokhtar (2015), *Cybersecurity: Can You Avoid Polish Electronic Puppets?*, Events Trends Magazine, Issue 6.

8. Nikita Reddy & Ogundar Reddy (2014), *Examining Cybersecurity Challenges and Emerging Trends in Cutting-Edge Technologies*, International Journal of Engineering and Technology, UK, Volume 4 N^o.1.
<https://doi.org/10.48550/arXiv.1402.1842>
9. Noura Al-FadaChellouch (2018), *The Threat in Cyberspace: The Inverted Threat to State Security*, Journal of the Babylon Center for Humanities, Volume 8, Issue 2.
10. Sarah Gordon & Richard Ford (2019), *Cyberterrorism*, Computers & Security, Volume 21, Issue 7. DOI: [10.1016/S0167-4048\(02\)01116-1](https://doi.org/10.1016/S0167-4048(02)01116-1)
11. Steve St. Clair (2011), *An Overview and Analysis of Cyberterrorism*, School of Doctoral Studies European Union Journal, Issue 3.

Reports:

1. European Commission (2020), *Cybersecurity: Our Digital Hub: A European Perspective*, Italy: European Commission, Joint Research Centre.
2. International Telecommunication Union. LO, December 28th, 2019.
3. https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-ar.pdf
4. Jiří Havlíček (2012), *The Threat of Cyberterrorism*, Report of the International Affairs Association (NATO), Prague Student Summit /1 -16, Model Nato 1-1.
5. Presidency of the Council of Ministers (2013), *National Strategic Framework for Cybersecurity*, Italy, European Union Publications Office.

Seminar article:

1. Duić et al., (2017), *International Challenges of Cybersecurity*, 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
2. DOI: [10.23919/MIPRO.2017.7973625](https://doi.org/10.23919/MIPRO.2017.7973625)

Internet websites:

1. Clive James (2016), *Cybersecurity - Threats, Challenges, and Opportunities*, American Society for Cybersecurity, on: www.acs.org.au, last access 2024.