Tạp chí Lý Luận Chính Trị Và Truyên Thông

Tạp chí điện tử tiếng Anh - Tập 31, Số 2 (2025)

Ngày nhận bài: 27/07/2025 | **Ngày phản biện:** 10/08/2025 | **Ngày xuất bản:** 25/10/2025

Tác giả: Thuy Hong LUU (Academy of Journalism and Communication)

1. An approach to impact analysis and research methods

In international relations research there are many approaches to impact analysis of which there are two notable methods.

The first approach to impact assessment is by analytical levels. It is one of the most common approaches that many international relations researchers are interested in and employ. According to this approach, there are three levels of analysis: individual analysis, country analysis and systems analysis(1). This approach is used to analyze the impact of cybersecurity issues on international relations. It considers the impact at three levels. First, individual analysis of cybersecurity issues as they affect individuals, especially officials, political circles and leaders who thereby affect foreign policy. Second, analysis at the national level where the impact is on national identity, specifically the values of the country in terms of culture, politics, etc. This affects the formation and implementation of foreign policy. And third, at the system level is the analysis of the impact on the relativity of forces, the shaping of the world order, and development trends of international relations.

The second approach to assessment and analysis of impacts is according to the nature of international relations. International relations is the interaction between subjects in many fields that cross national and territorial borders for the purpose of national interests. These interactions can consist of two states of cooperation and struggle. Research on the impact of cybersecurity issues on international relations will be analyzed according to the levels of status and the results of that relationship status.

This article will choose the second approach because the first approach is more suitable for analysis and assessment of foreign policy. The second approach,

although entering into the nature of international relations in impact analysis, is somewhat simple, so although the author primarily uses the second approach, it is still intertwined with the first approach during the analysis. The author uses specific analytical methods including: a case study method with examples in some specific situations; a survey and statistical methods to find data related to security issues; networks; and analytical methods.

2. An introduction to the problem and research situations

The 21st century is considered the "high-tech" century and the era of the internet, cyberspace and the emergence of social networks. According to a 2022 report of the corporate website "We Are Social" in the United Kingdom, at the moment the number of internet users is quite large, accounting for 62.5% of the total world population as shown in the table below.
Source: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper- growth-2/

With the growing number of online citizens, cyberspace has presented a special opportunity to cybercriminal groups of various sizes and levels of skill to exploit. The insecurity caused by cybercrime in cyberspace is known as a cybersecurity problem. So far, the impacts of cybersecurity issues on each individual and each country are quite clear. But how they affect international relations and the environment for development of a country is a question that needs to be answered. Therefore, research on this subject becomes urgent and necessary.

Currently, there is much published research on cybersecurity and cybersecurity issues. These resources include Milton Mueller, Andreas Schmitdt, and Brenden Kuerbis' "Internet Security and Networked Governance in International Relations (2014);" David S. Wall and Matthew Williams' "Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing" (2014); David Dittrich and Gregory Carpenter's "Hacking Back: Offensive Cyber Counterintelligence" (2015); Hồ Chí Minh National Academy of Politics'

"Unconventional Security: Theoretical Problems and Reality" (2015); Prof. Tran Dai Quang's "Cyberspace – Future and Action" (2017); Brendon Valeriano and Ryan C. Maness' "International Relations Theory and Cybersecurity – Threats, Conflicts, and Ethics in an Emergent Domain" (2018); V.K. Nguyen's "Cybersecurity Issues in International Relations in the Era of Industrial Revolution 4.0" (2018); and Viet Lam Nguyen's "Cooperation and Struggle on Cybersecurity in International Relations: Opportunities, Challenges and Policy Recommendations for Vietnam" (2020). The above works have put forward views on cybersecurity hidden beneath the correlation between cyberspace and national security, with national sovereignty, national interests, development projections and suggestions for the future to protect cyberspace or the content, the status, as well as consequences and solutions to the problem of high-tech crime and cybersecurity. There are works that review cybersecurity in international relations along with other international relations theory or consider cooperation and conflict in international relations on cybersecurity. However, analyzing the impact of cybersecurity on international relations from the perspective of international relations has not been clarified.

3. The concept of network security as a subject of non-traditional security

In the context of the strong development of cyberspace with the introduction and existence of indispensable digital tools for the new generation of people, such as email, social networks, e-commerce, chat, KOL, online games, e-sports, platforms, e-books, live stream, online meeting, online learning and so on, cybersecurity was born to ensure these tools are safe for netizens – internet users. Therefore, it can be understood that "Cybersecurity is the assurance of safety to people, the country and humanity against risks and challenges on the internet (cyberspace)." Appearing on the internet, these risks and obstacles also known as "cybersecurity issues," are being carried out by criminals with harmful intent to internet users.

Crimes in cyberspace are quite diverse, and can be classified into some typical categories. 1) High-tech crimes of intrusions and attacks toward databases; creating, spreading and developing virus programs, stealing of data and information, attacks of distributed denial of service (DDOS), illegal use of data, and undisclosed and unauthorized use of information found on the internet. 2) Traditional crimes in

cyberspace including property fraud such as using malicious code to steal email addresses, credit card information and personal information such as names, addresses, account passwords, phone numbers, social security card numbers, fraud through advertising, online sales, theft such as money theft from credit cards and accounts, embezzlement, money laundering by transferring money from stolen funds to e-money accounts and money transfer through apps like Western Union, etc., drug trafficking, prostitution including spreading pornography, criminal infringement on intellectual property rights, gambling, buying and selling stocks online, evading taxes, and personal terrorism crime (2). 3) Crimes directed towards a country such as: sabotaging or threatening the safety of national infrastructure systems such as power transmission systems, communication systems, control systems, and air traffic control (3), acts of a terrorist nature to exert pressure on the country or the whole society of a country in order to achieve political, religious, or ideological purposes with foreign elements and other acts such as cyber espionage, cyber attack, cyber conflict, cyber war, etc.

These bold and increasingly sophisticated activities are difficult to detect and handle. Cybercrime has become a major non-military challenge for many countries and a non-traditional security issue that needs to be monitored and addressed. Since then, the issue of network security has become an important factor in international relations.

4. The impact of cybersecurity issues on international relations

First of all, the issue of cybersecurity has forced international relations researchers to understand and clarify the content and nature of newly emerged terminology such as cyber sovereignty, jurisdiction in cyberspace, cyber border, cybergate, cyber border guard, cyberwar, cyber intelligence, cyber espionage, and cyberterrorism in international relations theory. The addition of research objects of international relations theory can also create new approaches to the world and international relations. This can change the thinking of leaders in countries from which the domestic and foreign policy changes, leading to changes in their behavior establishing international relations. In addition, because of the new terminology, there are also different views leading to different interpretations, different policies and different behavior in international relations. For example, on the issue of cyberwarfare,

Russia defines "Cyberwarfare is a confrontation between two or more states in cyberspace with the aim of damaging systems, processes and resources, information as well as other important structures, sabotaging the political, economic and social systems, influencing people's psychology to cause instability in society and the state, even forcing the state to make decisions in favor of the opposition." Meanwhile, the European Union has stated that: "Cyberwars are "virtual military operations" that can cause severe consequences both in civil and military aspects and will be part of future wars"(4).

Cybersecurity issues affect the basic attributes of the country such as national sovereignty and national interests. National sovereignty is understood as the supreme sovereignty of the country within its territory and the sovereignty of the country in international relations. However, when there is a cybersecurity problem such as a cyber attack or cyber espionage, it is quite difficult to determine to which country this cybersecurity problem belongs because the established information area, storing, processing, and exchanging anywhere in cyberspace is not limited to a specific physical geographical area, whether or not that country has sovereignty over the infrastructure in cyberspace. Therefore, the issue of cybersecurity leads to legal conflicts over the jurisdiction of the country in international relations. It also means that it is necessary to add the content of national sovereignty – national sovereignty in cyberspace or cyber sovereignty with the consensus of countries in international relations. The second is the national interest – the national interest is the realization of three goals: national security, development and influence.

With that in mind, at present, national security is being deeply affected by cybersecurity issues. Specifically, every year, thousands of large and small attacks on computer systems, social network accounts, and so on, affect the quality of life of netizens because they are in reality, also citizens of the country. More and more large-scale attacks on the national electrical, water, and storage systems affect the security of the country and even the very existence of the nation. In addition, the issue of cybersecurity is forcing countries to develop their scientific and technological capabilities and internal laws related to cybersecurity. This is the foundation for promoting the development of cyberspace in a more organized and ordered manner,

while also creating a safer environment for e-commerce and the network economy, contributing to the development of the country in line with the trends of the present age. In addition, the development of hightech science, effective prevention and response to cybersecurity issues also brings advantages at the negotiating table, contributing to strengthening the country's position in the international landscape in the process of sharing information and experiences.

Solving the issue of cybersecurity is also considered one of the flags to rally forces in current international relations. For example, the United States considers solving cybersecurity issues such as cyberattacks, cyberterrorism, cyber espionage, etc., as a priority for the country. At the same time, it calls on other countries for additional support. In this process, the US supports, coordinates, helps and leads other countries through bilateral and multilateral agreements and treaties, thereby creating a foundation for forming close and lasting relationships between the US and its partners and allies.

Cybersecurity issues affect bilateral relations between countries in two stages: cooperation and struggle. First of all, the issue of cybersecurity encourages countries to cooperate with each other from a basic to a comprehensive level on the bilateral relationship channel. The world is witnessing a period of exciting development of bilateral relations that overcomes geographic barriers, the level of development or political regime, such as the signing by the US and China of the Zhenzhen Cybersecurity Agreement repressing commercial espionage in September 2019. Russia and China have been conducting regular dialogues on cybersecurity initiatives since 2009 within the framework of the Shanghai Cooperation Organization (SCO). The two countries have institutionalized cooperation through the signing of an agreement on cybersecurity on May 8, 2015(5). The United States and Japan cooperated through the addition of cybersecurity issues such as cyberattacks with the bilateral Security Treaty during the 2+2 meeting between the Secretary of State and Defense Ministers of the United States and Japan in Washington in April 2019. Vietnam and the US signed a Memorandum of Understanding (MoU) on cooperation in preventing and combating transnational crimes, including high-tech crimes in 2019. The US and Singapore signed a Memorandum of Understanding (MoU) to expand cooperation on security in August 2021. Vietnam and Japan promoted bilateral

cooperation when signing a Memorandum of Understanding (MoU) on enhancing cooperation in the field of cybersecurity in November 2021.

In addition, there are many talks, seminars, discussions, and experience- sharing sessions, sharing views and coordinating actions to ensure network security, for example, in 2019 Vietnam and the US had two meetings on strengthening cooperation in crime prevention and control in general and high tech crime in particular. The talks between the US and South Korea from 2018 to 2020 resulted in joint statements and have led to a very close cooperation between the two countries. In 2021, at the meeting between India and New Zealand, the two countries agreed to cooperate more closely in the field of cybersecurity and cybercrime(6). The Defense Ministries of Lithuania and Poland held talks in May 2022 agreeing to strengthen cooperation on cybersecurity and set up a bilateral working group.

Cybersecurity issues are also a factor that creates differences of opinion, even conflicts and struggles between countries in international relations, in which the struggle to determine jurisdiction and sovereignty to resolve cybersecurity issues is common. As analyzed, cybercriminals are taking advantage of cyberspace, which has not yet been clearly defined, to commit crimes, leading to conflicts over jurisdiction, and disputes over territorial sovereignty in cyberspace between countries. Moreover, sometimes the issue of cybersecurity is an excuse for countries to accuse each other of increasing tension in international relations. The case of the US and Russia is an example. On the White House website, the Statements and Announcements section makes it very clear that "The Biden-Harris administration has repeatedly warned about the possibility of Russia engaging in malicious cyber activity against the United States in response to unprecedented economic sanctions that we have imposed"(7).

Cybersecurity issues affect the process of forming and perfecting international multilateral institutions. Cybersecurity is a transnational non-traditional security issue that not only affects citizen and national security but also affects regional and world security. According to information from Interpol, in the ASEAN region, police identified command and control servers that spread various types of malware, resulting in the discovery of nearly 270 compromised websites, including including government portals(8). In economic terms, the damage caused by cybercrime in the world will

amount to 6 trillion US dollars by 2021(9). Therefore, in order to prevent, avoid, combat and solve cybersecurity problems, it is mandatory for all humanity to join forces. Cybercriminals with attacks of various sizes and levels have forced countries to find solutions through multilateral diplomacy. Multilateral agreements and treaties related to cybersecurity are signed.

The EU is an example when it comes to many related international treaties, of which the Convention on Cybercrime signed on November 23, 2001 is the first international treaty on internet crimes and computer networks, in dealing with piracy, computer-related fraud, child pornography and cybersecurity violations, with the main objective of pursuing a common criminal policy to protect society against cybercrime, particularly by passing appropriate legislation and promoting international cooperation (10). In August 2002, the Organization for Economic Co- operation and Development (OECD) in August 2002 adopted Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. NATO also has made many responses to cybersecurity issues, including in 2016 when NATO heads of state and governments signed the Cyberspace Defense Pledge. In 2019 the United Nations General Assembly passed legislation on "Combating the use of information and communication technologies for criminal purposes." On that basis, the United Nations decided to negotiate to hold an International Convention Against Cybercrime with a negotiation period from 2022 to 2024.

In addition, agencies, organizations, and units that coordinate among countries have established international institutions on cybersecurity. Interpol's Computer Emergency Response Team (CERT) was created to help countries and individuals respond to computer emergencies. In July 2018, under the sponsorship of the Government of Singapore and the ASEAN-Japan Integration Fund, it established a mechanism related to ASEAN Cyber Capability Desk to be renamed by 2020 to ASEAN Cybercrime Operations Desk with the objective of assisting countries in the region to tackle cybercrime by using and developing intelligence, supporting investigations and coordinating operations, helping to connect law enforcement agencies with the private sector and other partners. Recently 49 countries in Africa collaborated to form the African Joint Operation Against Cybercrime Project (AFJOC),

which has been in operation since January 1, 2022. Within the timeframe of March 8, 2021 to February 28, 2023 African participants will promote coordinated actions against cybercrime in their member countries(11). In addition, Interpol's Cyber Fusion Center (CFC) was established with the aim of bringing together cyber experts from law enforcement agencies to collect and analyze all information about criminal activities in cyberspace to provide countries with intelligence. Or in February 2018, NATO established a Cyber Operations Center (CyOC) as part of NATO's SHAPE Command Structure, with the aim of integrating the allies' cyber capabilities into NATO military operations. At the 2021 NATO Summit in Brussels, the Allies adopted a new Comprehensive Cyber Defense Policy(12).

Cybersecurity issues are having a significant impact on international relations from hour to hour, day to day. Recognizing those impacts plays a role in guiding the policies and behavior of each country in the international landscape. A country like Vietnam that is developing strongly in the context of the international relations environment with its continuous and unpredictable fluctuations due to factors including cybersecurity issues, the important handling of the situation and effective and reasonable communication with partners and cyber challenges is essential to ensure the national interests./.

Tài liệu tham khảo

(1) See also Hoang Khac Nam, Theory of international relations, World Publisher.

(2), (3) See also, Ta Ngoc Tan (2015), Non-traditional security, theoretical and practical issues, Political Theory Publishing House, pp. 287-288.

(4) Prof. Tran Dai Quang, Cyberspace – Future and Action, p. 89.

(5) https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018 /816711/hop-tac-va-dau-tranh-ve-an-ninh-carry-in-quan-he-quoc-te-%C2%A0co-hoi %2C-thach-thuc-va-de-xuat-chinh-sach-doi-voi-viet-nam.aspx

(6) https://government.economictimes.indiatimes.com/news/secure-india/india-new- zealand-agree-on-close-cooperation-in-cybersecurity-cybercrime/87771225

(7) https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/ 21/fact- sheet-act-now-to-protect-against-potential-cyberattacks/

(8) https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations

(9) https://cybersecurityventures.com/hackerpocalypse-cybercrime-report- 2016/ (10)

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatyn

um=185

(11) https://www.interpol.int/Crimes/Cybercrime/Cybercr

ime-operations/AFJOC-

African-Joint-Operation-against-Cybercrime

(12) https://www.nato.int/cps/en/natohq/topics_78170.htm