International Conference Restructuring and Transforming Law 2026
Volume 5, Issue 1, July 2026
e-ISSN :2963-931X
icrtlaw@ums.ac.id

Cybersecurity from International Perspectives: The Cases of the UN and EU Initiatives

Prof. Dr. Önder KUTLU
Necmettin Erbakan University, Faculty of Political Science, Head of Department
okutlu@erbakan.edu.tr

Abstract

Cybersecurity as a global phenomenon has been on the agendas of international organisations for not only making policies but also keeping and maintaining tranquillity of nations. The nature of the subject imposes joint efforts of actors and defining policies at international level. The paper deploys the UN and the EU cases to shed light on their involvements in cybersecurity in terms of history, principles, means and mechanisms. The cases provide invaluable lessons for nation states and international organisations as the subject area has witnessed growing concerns with the advancements in technology as well as criminalisation of the area by mischievous behaviours of the criminal actors.

With the increase of awareness in the public about security concerns and the devastating effects of cybercrime, policy makers at national and international levels intend to pay attention to the issue. Hence, the consequences have wider implications in the public and in every actor in the society. Therefore, joint efforts should best be orchestrated by deliberate activities of international organisations. The two cases have their own histories and priorities. In addition, their special mechanisms and means are forward oriented and could guide member states in their activities.

This paper examines cybersecurity with its international dimension and finds that these unique cases set a blueprint for other organisations and nations to follow. The UN, for this purpose, has adopted the Sustainable Development Goals (SDGs) in respect to cybersecurity applications inter alia other purposes. This has alleviated the reception of the problem as sustaining the development of goals which are generally accepted proposals for the entire humanity, while the EU has concrete and effectful policies and organs to facilitate cybersecurity arrangements. The cases hint that development of cybersecurity studies influences general atmosphere in which every public policy actor (re)acts. So, without international level activities and provisions, national endeavours would have limited impacts.

Keywords: Cybersecurity, the UN, the EU, international organisations, cyber governance

I. Introduction

As an international issue, cybersecurity has attracted a wide range of responses from major intra-national, international and supra-national organisations. Being the one and only representative institution of entire sovereign states, the UN and a democratic union of the European states the EU have launched various mechanisms and means to deal with the issue at global and regional levels respectively. Their interests in the problem would have implications mainly on member

states but not limited to their realms of interests. Hence, the institutions would certainly have the prospect of highlighting the subject matter for global, regional and local commodities.

Intrinsically, cybersecurity is an issue that revolves around cross-national and cross-border breaches of law due predominantly to the deployment of internet and other IT facilities. In addition, it can contain certain national propositions, but at the same time there would be a great deal of international dimensions. It is often taken by these organisations as a crime prevention activity at macro level rather than a matter that promotes the prosperity of individuals at micro settings. The latter is chiefly laid upon the concerns of national governments.

The propositions of both the UN and the EU would have the prospect and aim of setting the standards for global and regional levels and therefore there could form a convenient ground for security implications on cyber networks. Besides, this common ground can be easily entrenched to international disputes and problem areas. The nature of cyberspace necessitates cooperation, collaboration and cohabitation: Geographical boundaries do not match the limits of cyber activities and crimes.

This paper expects to explore the UN and the EU cases. The examination of the UN initiatives will also include Sustainable Developed Goals (SDGs) issued by this organisation to propose a concrete model in dealing with national and international dimensions together. This seems to alleviate the drawbacks of general, abstract and theoretical policy discussions, rather it may focus on implementation of cyber policies in practice on solid grounds. The SDGs have implications in every state and every political entity as the goals cover national and international political and social matters.

The evaluation of the EU policies and mechanisms is also interesting as the Union has been able to provide certain success stories in promoting security of cyberspace. Combination and nature of the EU pose invaluable examples not only for the member countries but also for others which would exhibit interests in the case. The level of cooperation and coordination among member states and the facilitation of the EU in due process might grant a convenient atmosphere for other inter-intra national institutions and unions. Therefore, the contribution prompted by any type of organisation and any state is a right step in the right direction. Every state must have a cooperation mindset to fight against cybercrime and eventually have a safe ground for national interests.

The paper evaluates these two cases to form a framework for cybersecurity studies. This would provide a contribution to cybersecurity field both national and international levels, as both stages are intertwined. Consequently, national and sub-national studies would benefit from the international dimension.

II. Nature of Cybersecurity at International Level

The concept cybersecurity is relatively a new phenomenon. Therefore, an evaluation of the concept would bear fruitful results. For this purpose, it might be wise to breakdown the components of the word and eventually combine the two meanings to understand the issue properly. Oxford dictionary defines '*cyber*' as "*connected with electronic communication networks, especially the internet*". Anything related to electronic communication networks is seen as cyber, while '*security*' refers to "*the activities involved in protecting a country, building or person against attack, danger, etc.*". 'Cybersecurity' incorporates the "*measures that are taken to protect against the criminal use of electronic data*".

Cybersecurity is essentially a global phenomenon, because it involves cyberspace and atmosphere and therefore nearly every person, organisation and state is subject to cybersecurity concerns. The definition of 'criminal use of electronic data' may apply nearly every aspect of life: Data protection, digital surveillance, ethical issues, financial transactions, social interactions, etc. Therefore, all these areas are within the realms of cybersecurity and essentially there must be a deliberate public effort by governments initiating reflective measures to protect criminal deployment of electronic data.

Modern day human beings and organisations have got certain dispositions as such increased use of social media platforms, large scale transfer of financial assets, increased pace of human mobility, interdependency on nations/organisations, demanding public approaches, advancements in technology and dependency on electronic apparatus, and global political issues like environmental problems, organised crime, and human rights abuses. These dimensions necessarily put cybersecurity at the priority of individuals, communities, nations as well as international actors.

Internationalisation of cybersecurity owns essentially on globalisation in general terms. Local, regional and national problems and issues are transferred through globalisation to international levels. So, solutions of the problems should also be sought at international circles. Globalisation at the current pace has been hindering small scale problems at national borders. Instead, global and common solutions are preferable as the tools and means should also bring global perspectives. The points discussed below are basically the outcomes of globalisation. In addition, more can be added to the list of the factors referring to the global character of the subject matter.

First, social media platforms have been facilitating the globalisation (and spreading) of cybersecurity both in positive and negative ways. Internet addiction and social media platform dependencies pose a real threat to human beings in this account. Although the news related to misuse of social media circles have been evident among the traditional and the new media spheres, the users seem not to take any kind of actions to protect their privacy. Sharing confidential information with the public, for instance, appears to be a routine activity of individuals. Eventually, the number of child abuses and paedophilia cases have been increased dramatically in recent years. According to UNICEF (2024) data, 'About 90 million children alive

today have experienced sexual violence' and 'Close to 550 million children (around 1 in 4) live with mothers who are victims of intimate partner violence'. Yet the public does not intend to take the lessons of the news. Data protection and public surveillance issues do not properly attract the attentions of the public anymore. Instead, individuals are so eager to share data and information which are strictly confidential. In many cases, cybercrime is facilitated and maybe encouraged intentionally or unintentionally by the victims (Mandal, 2024; 161-163). This exhibitionist behavior is evident not only among the youth but elderly people who voluntarily facilitate breach of their own private sphere. Moreover, internet addiction is evident even among the children at primary school institutions. This puts individuals and society at danger, because human beings usually do not see any threat in sharing information, on the one hand, but encountering risky circumstances stemming from this display culture, on the other.

Second point to elaborate with regards to cybersecurity concerns is that the rocketing of financial transactions by the people in the street especially after the Covid-19 pandemic. Online solutions, including financial matters have been widespread among individuals and organisations. This poses a real hazard for the public. Many cybercrime cases are directly related to financial aspects. Council of the European Union claims that the global annual cost of cybercrime reaches €5.5 trillion (2026a). This is a potential risk area. Online gambling sites have been mushroomed, and international money transfers have exponentially increased recently. Many people prefer online shopping sites at national and international markets. Therefore, international money and goods transactions put international cybersecurity issue to the shore.

Third dimension is linked to human mobility and international migration cases. Legal and illegal border crossings could bring travel security issues together. Illegal and compulsory immigration accounts a worst picture as millions of people cross the border points without security checks and clearances. According to UN Tourism (2026), 1.52 billion people travelled internationally in 2025. Adding to this, national level tourism activities signify billions of tourists every year. Increased mobility reflects cybersecurity concerns as personal data and privacy are put at stake. This also bears consequences on migration, travelling for educational or health purposes. Besides, international travel business would make national problems international. The number of the countries taking place in tourism sector directly affects the scale and scope of the cybersecurity fears: The more the number the much the concern for cybersecurity.

Fourth factor to promote international involvement is the flexible interpretation of state sovereignty. The concept has been transformed completely since the time of Thommas Hobbes, the C16th, but the current interpretation of the idea needs to take differing and contrasting explanations. International organisations, for instance, play a major role in undertaking certain state responsibilities that has never been thought before. National governments are forced to make generous concessions for the favour of international actors. For example, adoption of prevailing jurisdictional role of European Court of Human Rights by Turkish government in 1987 was a turning point towards an international court taking over certain responsibilities from the national institutions of Türkiye (Council of Europe, 2026). Therefore, international atmosphere

is in favour of international organisations in the forms of environment, human rights and crime-related policies.

Fifth dimension is about the advancements of international organisations that would ease the classical and traditional responsibilities emanated from national jurisprudences. As the disputes and fragmentations among nations increase these organisations have advanced to fill the vacuum left by national actors. International organisations play new roles and undertake further responsibilities as the time pass by. The UN, for example, resembles a federal state by having judicial, executive and legislative functions. The EU is no different as its institutions and organs match nation states, including parliament, commission and council. This makes these organisations state-like institutions often sharing their roles and fulfilling the tasks that used to be located at nation level politics.

Sixth, *advancements in technology and dependency on technical apparatus* make individuals and states more vulnerable to cybercrime. Technology has pros and cons. On the one hand, it facilitates administrative mechanisms and application of policies, on the other it may be open to malicious cyber-attacks. This has also international aspect as internet pave the way for international fraudulent initiatives. Hence, international efforts to provide safe internet is vital for national governments.

Final, global politics requires carefully planned and implemented international undertakings to pay special tribute to cybersecurity. Global political issues such as money laundering, drag trafficking, terror, environmental problems and human rights abuses all have a certain degree of international communication and cooperation. Therefore, international organisations feel obliged to make efforts to extinguish cybercrime by providing moral support as well as concrete mechanism and policies to deal with.

III. International Organisations

International organisations, especially the ones with global interests pay attention to global problems. Cybersecurity is not an exemption. The UN and the EU have wide ranges of concerns related to regional and global issues. Cybersecurity policies and crime-related preventive measures serving the needs of global network have been provided predominantly by these two organisations. So, this section evaluates the UN and the EU with the intention of spelling out their contributions to cybersecurity.

A. United Nations

Being formed after the WWII, the United Nations has been serving as a global state with responsibilities that normally a nation state undertakes. Organs and institutions directly and indirectly affiliated to the UN with responsibilities in terms of financial, social, cultural, and political tasks operate under the umbrella of the Union i.e. WHO, ILO, FAO, UNDP. (Kutlu, 2025; 40-42). They enjoy the freedom to serve international community with a degree of

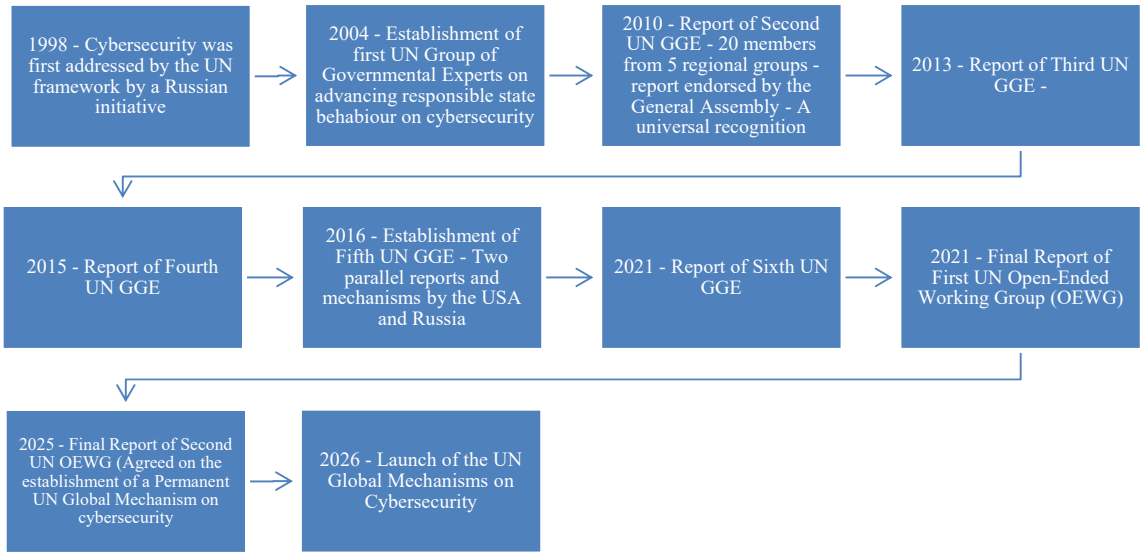
autonomy. This makes them reasonably professional organisations. These tasks also include cybersecurity in general terms.

This part examines the position of the UN in the terms of cybersecurity. First, history and development of cybersecurity evaluated; second, breach of security, namely crime dimension of the issue examined; and final, the meanings and implementation of security through the UN SDGs, which are to promote welfare and better living conditions for human beings are addressed. So, positive and negative dimensions of the issue are discussed by evaluating criminal and social implications sides at the same time.

a. Evolution of a global cybersecurity mechanism

The year 2026 signifies a turning point in establishing a global mechanism as a part of the UN mission. The figure below summarises the interests of the UN by obtaining the task in an evolutionary pace. The initiative has been discussed and disputed by the UN since 1998, when Russia proposed a framework for cybersecurity with the prime intention to fight against information asymmetries and information wars. The figure displays that it has taken nearly three decades to finalise a global policy and a network to establish at the UN level.

Figure 1: History of UN cybersecurity governance



Source: Rupp, C. (2026). 'The UN's New Global Mechanism on Cybersecurity'

The main process and the outcomes are summarised (Rupp, 2026: 5) below:

- 2013: International law would apply to cyberspace. In 2021, specifically affirms "that international humanitarian law applies only in situations of armed conflict",
- 2015: 11 voluntary, non-binding norms for responsible state behaviour in cyberspace.

- 2021: Ten principles on cyber capacity-building (CCB) by which states are guided by in relation to State use of ICTs in the context of international security,
- 2022-2024: A set of eight universal cyber CBMs, encompassing inter alia a global Points of Contact.

By having established an internationally recognised binding mechanism in cybersecurity as a part of international law the UN system have been able to obtain a powerful instrument. The applications of the principles signalled important milestones of the process. The pace of the developments highlighted above shows that it has been a difficult process that member states proposed conflicting demands in shaping and designing a global mechanism to supervise cybersecurity initiatives. Besides, the period has witnessed also a transformation in cybersecurity issues as cyberattacks have become sophisticated in the scale and scope. During the 28 years period from the beginning to the end the initiative experienced so many developments and conflicts of interest. Establishment of the Global Mechanism has been a revolutionary achievement as this is a part of the UN mission and affect the global networks. Despite the criticisms for the UN (in)existence and (under)performance on global conflicts, the availability of the mechanism even after 28 years is a self-explanatory achievement.

The UN involvement initially started with the attacks from malicious circles to undermine its digital systems and manipulate data stored in the UN institutions (The UN, 2021. 1-2). This is also the case of national governments and private companies. The uniqueness of the UN case is that the organisation comprises vital responsibilities vis-à-vis member states and other international organisations. It is even argued that 'the cybersecurity incidents go beyond system disruption and may affect mandate delivery' (The UN, 2021: 2). This concern/fear seemed to trigger a series of initiatives initially to secure their structures and operations and eventually setting up a security mechanism for international community.

b. Principles of the UN and the Convention Against Cybercrime

Having examined the organisational structure and policies of the UN, the Joint Inspection Unit Report of 2021 (pp. 21-50) lists 11 recommendations to establish a sound resilient cyber structure. They include:

- Engaging with legislative and governing bodies
- Embedding cybersecurity into organizational risk management
- Building on the convergence between physical security and cybersecurity
- Shaping regulatory frameworks for compliance and accountability
- Harnessing the contributions of oversight mechanisms
- Instilling a cybersecurity culture from the leadership down
- Implementing a whole-of-organization approach
- Establishing the workforce as a first line of defence
- Optimizing financial resource allocation for cybersecurity
- Investing in dedicated and specialized human resources

- Reflecting and reporting on organization-wide efforts towards improved cyber resilience.

These measures are aimed at establishing a system that can successfully form a defending mechanism against cybercrimes. This includes strengthening the body and improving its relations with surrounding factors.

This paper is designed to pay attention much on the UN role in commissioning a cybersecurity network and security assurances for independent states and other international actors. A robust UN is vital for the global system, but the organisation's role and mission of establishing a fair and flexible environment for the states to operate is equally important, if not more. The position of the UN is not like any other international organisation. Therefore, its weaknesses and strengths are closely monitored by the global community. Moreover, once the UN system operates properly, the relations among member states would be stable and fair.

The mission of the UN is that through establishing a convention related to cybercrime the organisation proposes to set a blueprint and framework for the states to follow. The legislations are often directed and affected by the outcomes and offsprings of criminal activities. So, the UN General Assembly issued a convention to fight against criminal acts and therefore this would organise and regulate the policy area. This resembles the development of human rights when the abuses are evident policy makers would think about the ways of preservation and protection of human rights. Therefore, at the General Assembly meeting on December the 24th 2024, the UN proceeded a binding decision: 'United Nations Convention against Cybercrime' (2024). Obligations and regulations governing the area form the limits and priorities of the policy area. The convention contains 9 Chapters and 68 Articles. The Chapters include General provisions, Criminalization, Jurisdiction, Procedural measures and law enforcement, International cooperation, Preventive measures, Technical assistance and information exchange, Mechanism of implementation, and Final provisions.

Chapter I, General provisions section (6 articles) spells out the general context of the Convention by purpose, terms, scope, respect for human rights and protection of sovereignty. Chapter II, Criminalization section (14 articles) deals with the responsibilities of states in the terms of cybercrime types. Chapter III, Jurisdiction section (1 article) highlights jurisdiction issue. Chapter IV, Procedural measures and law enforcement section (11 articles) deals with scope of procedural measures. Chapter V, International cooperation section (17 articles) shape international dimension of cybercrime and security. Chapter VI, Preventive measures section (1 article) issues preventive measures in cybercrime. Chapter VII, Technical assistance and information Exchange section (3 articles) underlines technical issues. Chapter VIII, Mechanism of implementation section (2 articles) features Conference of the States Parties to the Convention, and Secretariat. Chapter IX, Final provisions section (9 articles) examines implementation of the Convention.

Of the content in the Convention, Chapter II sets out the scope of cybersecurity by pointing out the dimensions of cybercrime. Having done, the Convention poses a framework for analysis, as the criminalisation signifies the negative pace of the issue. The types of crimes underlined in the chapter include:

- Illegal access,
- Illegal interception,
- Interference with electronic data and information
- Interference with communications technology systems,
- Misuse of devices,
- Information and communications technology system-related forgery,
- Theft and fraud,
- Online child sexual abuse or child sexual exploitation material,
- Solicitation or grooming for the purpose of committing a sexual offence against a child,
- Non-consensual dissemination of intimate images,
- Laundering of proceeds of crime.

These aspects are also the phases of cybersecurity. In other words, taking counter measures to deal with these issues could create awareness in the public and therefore cybersecurity could be achieved in public and private organisations and individuals. Hence, they may be related to private and public domains. The mechanism and assurances prescribed by the Convention have formed an important cornerstone of cybersecurity as 'security' and 'crime' reflect the two sides of a coin. Studies on security help develop literature on crime and *vice versa*. Therefore, the UN interests by establishing of a mechanism to fight against cybercrime would certainly contribute to the enrichment of an understanding related to cybersecurity. As a matter of fact, the concept security has wider implications than crime, but the two concepts go together. In addition, undertaking a supervisory role of the subject matter as to the global scale by the UN signals an indicative role for other organisations and independent states to take concrete steps. The position of the UN is indicative of the global view in most of the global issues.

The formation of the UN Global Mechanism on Cybersecurity in 2026 would have to be in contact with the process and procedures of the Convention. The UN system is supposed to be working in communication with its sub-structures. The Convention and Global Mechanism must have a common ground to share data and have the prospect of synchronising their policies and activities. The implications and mandate of imposing certain responsibilities defined by the Convention would be accorded through the Global Mechanism on Cybersecurity. The breaches and misuse of security mechanisms mean crime soon as the breach is serious enough to undermine security.

The UN has also a role to orchestrate joint activities of international organisations for cybersecurity. This includes the promotion of national and international level cybersecurity mechanisms by providing a guide for national and international policy makers. The document titled 'Guide to Developing a National Cybersecurity Strategy'

(UN, 2026c) produced by the UN with the active contribution of 34 international organisations has a ubiquitous example of this effort. Some of the contributing organisations include World Bank, IMF, Interpol, UNDP, African Union (AU), Arab League, NATO Cooperative Cyber Defence Centre of Excellence, World Economic Forum, and the European Union Agency for Cybersecurity.

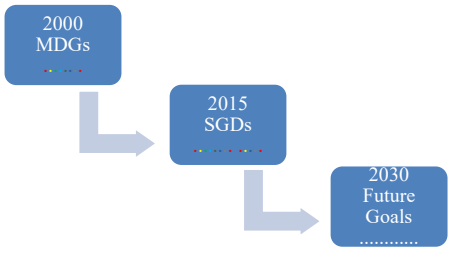
A bunch of the principles proposed by the Guide (UN, 2026c; 27-30) are as follows: "Comprehensive approach and tailored priorities, Inclusiveness, Economic and Social Prosperity, Fundamental human rights, Risk management and resilience, Appropriate set of policy instruments, Clear leadership, roles, and resource allocation, Trust environment, Technological foresight and adaptability". The Guide signifies a starting point for policy makers. The principles might seem not to be unique, but a common effort to promote the same principles could propose a shared set of blueprints for the nations to follow.

c. Sustainable Development Goals and Cybersecurity

The Sustainable Development Goals (SDGs) were introduced during the Sustainable Development Conference at the United Nations Conference in Rio de Janeiro in 2012 to replace the Millenium Development Goals (MDGs) of 8 areas introduced in 2000 (UNDP, 2026). MDGs were thought primarily to deal with poverty, while SDGs have been pointed to concentrate on wider propositions in social, cultural, economical and technical senses. By MDGs, the UN claimed to provide success in lifting extreme poverty by 1 billion people; increasing child mortality more than half, improving school drop numbers by half and falling of HIV/AIDS infections by almost 40 % for the last three decades (UNDP, 2026).

In September 2015, SDGs were introduced as the follow-up program of MDGs to increase the welfares of human beings. The introduction of SDGs has been evolutionary, starting from MDGs in 2000 to SDGs in 2015 and this plans to lead to the formation of Future Goals in 2030. This method has posed advantages as the process requires the support of sovereign states and it is not obtained overnight.

Figure 2: Development of SDGs



Source: UNDP, 2026, 'Background on the Goals'

MDGs included eight elements: Eradicate extreme hunger, Achieve universal primary education, Promote gender equality and empower women, Reduce child mortality, Improve maternal health, Combat HIV/AIDS, malaria and other diseases, Ensure environmental sustainability, Global partnership for development.

Figure 3: Millenium Development Goals

Source: UN, (2026a). 'Millenium Development Goals'

MDGs have been transformed to the SDGs as a next step of developments. An independent non-profit research centre, Oceania Cyber Security Centre (OCSC) proposed to evaluate SDGs with the intention of measuring their strength to support cybersecurity and found that every goal has the potential to affect cybersecurity, albeit varying degrees.

Figure 4: Sustainable Development Goals

Source: UN, (2026b). 'Sustainable Development Goals'

The Analysis produced by the centre (OCSC, 2022: 8-12) argues that the SDGs and their involvement with cybersecurity prevails certain dispositions: First, 'No poverty' indicates that "poorly designed technological products create space for cybercriminals to exploit market digitisation and undermine the economic benefits of ICT development". Second, 'Zero hunger' involves 'the technologies and computer systems

directly and indirectly involved in digitised food production need adequate protection from malicious actors who could disrupt production and distribution and consequently destabilise supply chains and generate food insecurity.' Third, 'Good health and well-being' is directly related to the SDGs as 'digital health services are vulnerable to attacks due to a historical lack of cybersecurity investment in the sector.' Fourth, 'Quality education' is threatened when data 'breaches are of major concern to educational institutions, but as learning has increasingly moved online or into hybrid arrangements, the instruments of teaching are also at risk.'

Fifth, 'Gender equality' could be linked by 'ICTs can open new opportunities to women, but they also present new avenues for cyberviolence and exploitation against women'. Sixth, 'Clean water and sanitation' is assumed that 'ICTs are a growing component in modern water facilities which are increasingly vulnerable to cyber threats.' Seventh, 'Affordable and clean energy' may be related to SDGs as 'technology enhanced grids are susceptible to cyber-attacks which can increase electricity prices and paralyse renewable energy sources and smart grids.' Eighth, 'Decent work and economic growth' is related as '…new technologies can boost economic growth, unfortunately they also open new avenues for cybercrime which can negate these benefits.' Ninth, 'Industry, innovation and infrastructure' is supposed to be dealing with 'Cyber vulnerabilities within improved infrastructure developments must be addressed in order to ensure that new infrastructure networks are resilient and functional.'

Tenth, 'Reduced Inequalities' deals with 'a digitally underdeveloped country with a high level of cyber inequality may lead to marginalised groups having a heightened vulnerability to cyber insecurity issues which further entrench inequalities.' Eleventh, 'Responsible consumption and production' is assigned to SDGs as 'the challenge within this relates to potential cyber-attacks against the systems responsible for consumption and production, such as waste management. Twelfth, 'Sustainable cities and communities', assumes that 'cities are often the target of cyber criminals and cyber-attacks can potentially disrupt key elements of city life such as police services, water, sanitation, energy and transport. Thirteenth, 'Life below water' involves, because 'cybersecurity is a key component in combatting Cyberpoachers' who operate in an unregulated online market and is therefore, integral to protecting marine life from the illegal animal trade.'

Fourteenth, 'Climate action' is important because 'cybersecurity is an important part of our efforts to stop climate change. It maintains vital critical infrastructure, including for example water supply networks and low-emissions energy systems, which help to reduce emissions and advanced resilience'. Fifteenth, 'Peace, justice and strong institution' involves as 'under educated and ill-equipped users are highly exposed to cybercrime.' Sixteenth, 'Life on land' section is prioritised and 'these technologies are vulnerable to cyber-attack which undermine their development contributions and

endanger native species.' Seventeenth, 'Partnership for the goals' is vital as 'underdeveloped partnerships challenge the effective governance of cybersecurity and are thus invaluable to achieving all the previous goals.'

Examinations of the SDGs – cybersecurity relations usually reveal that cybersecurity plays and important role in establishing resilience, security and sustainability of critical system and infrastructure. The evaluation proposed by Dede *et.al.* (2024) claims that SDGs positively contribute to the cybersecurity and *vice versa.* SDGs are to improve welfare and resilience of individuals and communities and in doing so quality of life increases.

According to Ige, Kupa and Ilori (2024; 345-346), technology deployment in public policy areas contribute to the establishment of direct support to the achievement of SGDs and underpin a broader ecosystem for sustainable development. The contribution may be by direct and indirect ways, but the provision of a sustainable environment, especially security concerns play pivotal roles in due process. The examination of SDGs given above shows that cyber space and its use for security arrangements help contribute general atmosphere. Besides, specific concerns on SDGs would be eradicated through cyber arrangements.

The UN involvement in development attempts would certainly assist in the global recognition of the principles. In addition, the utmost importance of cybersecurity in daily lives of individuals and institutions seems to direct international community to find ways of establishing direct ties with SDGs. Hence the global components of SDGs and the global effects of cyber space are supposed to be linked to obtain positive outcomes.

B. European Union

Being a democratic establishment and representing 27 sovereign states of Europe, the EU has got provisions for every aspect of a state in respect to public policy areas. During its history these policies have been evolved from coal and steel industries to common markets and common defence and foreign policies. The developments have been shaped by the collective efforts of member states and the organs of the Union. This has denoted a unique example originated by democracy and the rule of law. Such varieties and even hostilities among the members for relatively short period time, namely the remnants of the WWII have been converted adeptly to a federal or confederal state. Therefore, the process of policy aspects has been directly affected by certain developments. The pace of progression saw the deterioration of the Eastern Block or the demise of the Soviet Union, but the policy areas were not limited to economical or political agendas rather they had provisions for social, cultural and legal issues.

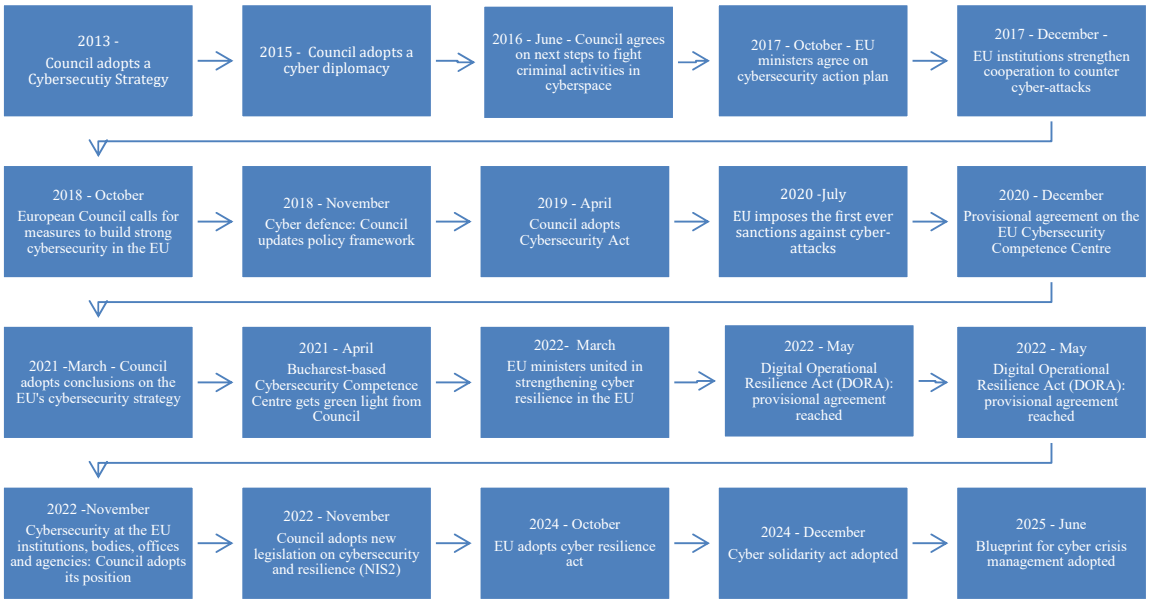
International Conference Restructuring and Transforming Law 2026
Volume 5, Issue 1, July 2026
e-ISSN :2963-931X
icrtlaw@ums.ac.id

a. Evolution of a European cybersecurity mechanism

The enactment of the Maastricht Treaty in 1992 forming the EU was the most important milestone of a union of states that resemble a state-like supra-national organisation with certain democratic concerns and priorities. The WWII was seen the worst war in the history of Europe, with millions of deaths and casualties. So, the post-war period triggered democratic consciousness in the international community as well as Europe. The UN was the international response to these demands, while the EU signifies the European reaction. The development of the Union witnessed a series of devastations and volatilities in global scale. Hence, the measures produced, and the advancements achieved and the contribution made in cybersecurity area own very much on to the EU policies and actors.

Figure 5 summarises the major developments achieved in due course. There are also so many steps which are decent to mention taken for the case of cybersecurity by different organs and actors of the EU i.e. the Council, Ministers, Parliament, and the Commission. The timeline indicates the European position as to cybersecurity. This shows that the EU has not only imposed bounding legal frameworks for its institutions but also promoted member state actions in a coordinated discipline. Although the pre-2013 period witnessed numerous cybersecurity measures by the EU, this paper is interested in the current position of the Union to be highlighted. Therefore, the post-2013 period is cited by Figure 5.

Figure 5: History of EU cybersecurity governance



Source: Council of the European Union, 2026b, 'Timeline - Cybersecurity' and Sachs, Schmalfeldt & Zettl-Schabatt, 2024: 4.

Figure 5 illustrates that the levels and contents of cybersecurity measures have been initiated by the pressure imposed through cybercrime incidents. The ontology of cybersecurity hints that criminal activities and misuse of cyber instruments have been the driving force as the drawbacks and the pressure from the suffering actors create a convenient medium for the policy makers at the EU and national level institutions.

Establishing a framework for member states and the EU institutions was not an easy task, especially in a topic like cybersecurity, because the subject matter has been subject to rapid changes on the one hand, and the member states, private sector and individuals are keen on liberal approaches to the issue, on the other. This seems to determine the founding principles of cybersecurity. Besides, cross-border and cross-continental dimensions of cybersecurity have also impositions on policy makers. As argued, the EU level activities would pose precious lessons not only for member states but also other states and international organisations. Despite the global position of the stakeholders as to cybersecurity, the central role of a democratic union like the EU could certainly signal a general charter to adopt.

b. EU Principles on Cybersecurity

The EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the new EU Cybersecurity Strategy (2020) to "answer to the challenges of geopolitical competition in cyberspace, and the increased cyber threat landscape, especially following the Covid-19 pandemic. It allows the EU to increase its resilience and show leadership in cyberspace; build capacities to prevent, deter and respond to cyber-attacks; and strengthen its partnerships in favour of a global and open cyberspace."

The strategy (2020, 1-4) reaches the following conclusions:

1. Transport, energy and health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on network and information systems that are increasingly interconnected.
2. The threat landscape is compounded by geopolitical tensions over the global and open Internet and over control of technologies across the whole supply chain.
3. The malicious targeting of critical infrastructure is a major global risk.
4. Concerns about security are a major disincentive to using online services.
5. The investigation of nearly all types of crime has a digital component.
6. Digital services and the finance sector are among the most frequent targets of cyberattacks, along with the public sector and manufacturing, yet cyber readiness and awareness among businesses and individuals remain low.
7. The EU lacks collective situational awareness of cyber threats.
8. Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information.

The background information given above would certainly reflect the mindsets of the actors at the EU. So, these provisions are to understand the strategy and the implementation practices of the Union. They seem to highlight the importance of the subject and the components of cybersecurity, surrounding

the atmosphere in which the member states and its actors operate. It claims that the EU has got awareness to fight against threats.

In addition, the strategy (2020, 4) proposes to issue concrete proposals on "three principal instruments –regulatory, investment and policy instruments". Three areas are as follows:

1. Resilience, Technological Sovereignty and Leadership
   1.1 Resilient infrastructure and critical services
   1.2 Building a European Cyber Shield
   1.3 An ultra-secure communication infrastructure
   1.4 Securing the next generation of broadband mobile networks
   1.5 An Internet of Secure Things
   1.6 Greater global Internet security
   1.7 A reinforced presence on the technology supply chain
2. Building Operational Capacity to Prevent, Deter and Respond
   2.1. A Joint Cyber Unit
   2.2. Tackling cybercrime
   2.3. EU cyber diplomacy toolbox
   2.4. Boosting cyber defence capabilities
3. Advancing a Global and Open Cyberspace
   3.1. EU leadership on standards, norms and frameworks in cyberspace
   3.2. Cooperation with partners and the multi-stakeholder community
   3.3. Strengthening global capacities to increase global resilience

Some of the concreate measures initiating the strategies highlighted in the document are as follows:

The EU should ensure:

- Adoption of revised NIS Directive.
- Regulatory measures for an Internet of Secure Things
- Through the CCCN investment in cybersecurity (notably through the Digital Europe Programme, Horizon Europe and recovery facility) to reach up to €4.5 billion in public and private investments over 2021-2027;
- An EU network of AI-enabled Security Operation Centres and an ultra-secure communication infrastructure harnessing quantum technology.
- Complete the European cybersecurity crisis management framework and determine the process, milestones and timeline for establishing the Joint Cyber Unit;
- Continue implementation of cybercrime agenda under the Security Union Strategy;
- Encourage and facilitate the establishment of a Member States' cyber intelligence working group residing within the EU INTCEN;
- Advance the EU's cyber deterrence posture to prevent, discourage, deter and respond to malicious cyber activities.
- Review the Cyber Defence Policy Framework.
- Support synergies between civil, defence and space industries;
- Reinforce cybersecurity of critical space infrastructures under the Space Programme.
- Define a set of objectives in international standardisation processes, and promote these at international level;
- Advance international security and stability in cyberspace, notably through the proposal by the EU and its Member States for a Programme of Action to Advance
- Responsible State Behaviour in Cyberspace (PoA) in the United Nations;

- Offer practical guidance on the application of human rights and fundamental freedoms in cyberspace;
- Strengthen and promote the Budapest Convention on Cybercrime,
- Expand EU cyber dialogue with third countries, regional and international organisations, including through an informal EU Cyber Diplomacy Network;
- Reinforce the exchanges with the multi-stakeholder community, notably by regular and structured exchanges with the private sector, academia and civil society;
- Propose an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board.

Regardless of their rate and success of implementation, these proposals would claim to reach the target as they not only involve with the EU level institutions and provisions but also national and third-party level activities. Besides, they offer providing assurances by regulatory activities, organisational dimensions and practical implications.

The success story of the EU owns much on to the establishment of a special agency in facilitating and carrying out through European scale and scope and contributing successful implementation of the policies. European Union Agency Cybersecurity (ENISA) (2026) was established in 2004 to "contribute to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure."

The structure and mission of the agency were revised in 2019 and given a permanent mandate (2019, ENISA, Article 3). The Agency has provisions for three types of actors: First, national/EU authorities; second, private sector; third, citizens. This implies that cybersecurity at the EU level would propose to regulate and produce improvisions on the actors at every level of societies. Being a comprehensive alignment, three components/segments of the EU governance could be covered by the Agency. The Agency would also play the role of a cybersecurity champion by empowering individuals, creating awareness and assurances for private sector and directing public authorities to pay attention in the protection and maintenance of security (See: ENISA website: https://www.enisa.europa.eu/). As an outcome of these tripartite relations, the Agency has provided documents on AI, Cyber hygiene, Digital identity and data protection, Risk management, Cybersecurity of critical sectors, Cyber threats, etc. The documents hint also the interest area of the agency.

Cyber Resilience Act (2024) was the last step taken for cyber space in 2024. The rather detailed act spells out the provisions of building a healthy structure vis-à-vis cybersecurity. The act has got 130 propositions, 71 articles, 6 annexes. This was intended to form a resilient institutional ecosystem.

The EU documents and policies are not easy to follow as the documents cover a wide range of areas. In this vein, "the EU's new Cybersecurity Strategy for the Digital Decade forms a

key component of Shaping Europe's Digital Future, the Commission's Recovery Plan for Europe and of the Security Union Strategy 2020-2025" would also be mentioned. The rules, regulations and documents are not limited to the mentioned papers. However, the documents displayed reflect the variety and depth of the subject.

c. Contribution of the EU to Cybersecurity Sphere

The EU involvement in cybersecurity varies from regulatory institutions to implementation and control of activities. This provision resembles a federation of European states structure. It owns very much on to the malicious activities of individuals and organisations, and the ambiguities surrounding the subject matter. Advancements in cyberspace and breaches of law in cyber activities seem to direct policy makers at national and international levels.

As a democratically motivated organisation, the EU has got to pay attention to the issue. For this reason, a series of actions taken by European policy makers. The strong institutional ties and organisational apparatus with a significant degree of expertise have directed the EU officials to invent means and ways for this purpose. The evolution of the EU sounds like resembling its achievements in cybersecurity. This experience may benefit national and international actors as well as private sector, individuals and civil society. Provisions of the EU are widely followed by member 27 states, candidate countries and civil initiatives worldwide.

In addition, there is also another private-public funded institution to deal with cybersecurity issues in Europe: European Cyber Security Organisation - ECSO (2026). This institution is a partner organisation of the EU. It was established in 2016 for "developing Europe's cybersecurity resilience and strategic autonomy, as the European Commission's contractual partner for the Public-Private Partnership in Cybersecurity". This has been a unique Europe-invented organisation to bring public and private dimensions together. The organisation consists of members from 30 countries, over 300 institutions at eight categories. This voluntary organisation has also associate members from outside of the EU, EFTA and the UK. The members are SMEs, Associations, Universities, research & technology organisations, and National public administrations. This signals an opportunity for partnership possibilities in cybersecurity.

The EU scale cybersecurity arrangements appear to take necessary measures for the implementation of its policies. Besides, the Union formed by the states which have closely knitted ties in terms of economy, society, politics and technology may set the scene for other international organisations and states. The networks among the member countries resemble a nation state with certain federal mechanisms. This may alleviate the effects of malicious efforts which present a real threat for every organisation and individual. By which, nation states and regional or international organisations might find ways of common policies and programs in obtaining security and fighting against criminally oriented practices.

IV. Cybersecurity: Lessons Learned from International Organisations

The evaluation of the cases taken indicates that cybersecurity as an international phenomenon requiring internationally coordinated efforts. The UN, representing international dimension and the EU, representing supra-national aspect have accumulated a great deal of rules, regulations and arrangements. So, their contributions are supposed to be greatly appreciated by member states and other national actors. Their roles in global politics might also affect their reception by respective organisations. Global politics, namely globalisation of national issues generalise domestic problems. The acceptance of international organisations as the actors of international law after the WWII was a starting point for these entities. For the time being, however, they have gone far away that was not initially dreamed of. The walk of the organisations has not reached their final destinations yet.

The evaluation also shows that international organisations are rather dynamic objects both in their institutional structures and policies. This has advantageous provisions, because the developments in international sphere require dynamic organisations. This is evident in the UN and in the EU. The UN has been severely criticised due to their political weaknesses and their lack of instruments to combat human rights abuses especially of the USA and its close allies (Kutlu, 2025). Yet, there is no alternative at least for the time being to fill the vacuum left by the UN. This is relatively a weak argument for the EU. By the same token, the EU would act like a federal state, especially in the cases where security concerns are high, i.e. cyber area.

The analysis reveals that cybersecurity is also a dynamic field with exponentially enlarging interests. The humanity has experienced a quantum leap in the area for the last decade or so. The advancements in AI have positive contributions to the wide-spread acceptance of this instrument. It has triggered lively discussions and curiosity whether the tool would get out of control or the information provided with the mechanism reflect the real data. Nonetheless, the jury is still out in the issue. There are pros and cons of the problem. Therefore, policy makers whether national or international levels feel obliged to produce measures to fight against the drawbacks and to promote the benefits stemming from the applications. Cybercrime is the main concern on the negative side, whereas the facilitation of the lives of individuals and the activities of organisations is on the positive side of the subject matter.

In democratic societies, major policies and instruments are usually prompted by negative developments, crises, chaos and catastrophic events. When the policies have reached a certain level of maturity, other concerns would help build sound structures and policies. The cybersecurity area is no exception. Breaches of privacy, abuses of human rights, interference of free market mechanisms, and other types of wrongdoings dictated national and international policy makers to act. When the problem is a global one, the solutions would also come from global circles. Therefore, the subject is an issue of global governance. Every actor may have a positive role in exterminating malicious intrusions. Cybersecurity requires joint efforts from not only official public policy actors but also from unofficial and often civil society institutions. Cyber character of the problem often requires cyber countermeasures.

In the UN case, the organisation has successfully integrated the SDGs to cybersecurity issue. This help enrich the content of the issue and taking it away from crime-related ties. There needed to be a positive story to connect the problematic issue to positive development proposals. As the SDGs are popularly supported by national actors and international stakeholders, the process of dissemination has avoided resistance from involved circles. The EU did not need these kinds of excuses/means nor they illustrated it under cover-ups. The difference is related to the needs for and the features convening it.

National governments would learn from the experiences of international or supra-national organisations as the problems resemble, the solutions are expected to match these similarities. Besides, involvement of world-wide-web (www) dictates cooperation and collaboration among every policy actor. Global governance contributes the orchestration of the efforts in the global scale, while national governance would direct national actors to come together.

V. Conclusions

The paper concludes that international involvement in cybersecurity is vital in finding adept solutions and in implementing the policies for this end. There is a consensus in literature and in the public that every individual and organisation are subject to cyberattacks and criminal assaults. Therefore, public actors feel obliged to carry out cybersecurity policies to deal with the discrepancies stemming from the use of internet. On the contrary, individuals are open to the exploitations of crime circles. This contradicting attitudes of the public and the risky practices by the part of cyber criminals must be brought to an equilibrium.

Besides, there is a growing awareness in the policy makers, at least in international scale to terminate or ease the problem. This might have been pushed by the efforts of national actors or international organisations. This is something open to dispute. But the availability of an alertness is a blessing. So that national and international actors cooperate and collaborate for the purpose. In addition, the network issue and multi-national involvement in cybercrime cases would have to face a powerful international organisation rather than dealing with the issue by nation states individually. Take the attitude of social media platforms as an example. They feel more powerful in the disputes with nation states than international organisations for commercial and political reasons. The same is true that the social media has multiple policies in respect to the states and organisations which may vary in economic, political and military strengths. Having done so, cybersecurity could be provided with a degree of confidence by the account of international actors.

The examination finds also that even though the initiation of cybersecurity stems from criminal acts, international organisations would eventually go beyond illegal activities for sustainable solutions. The SDGs could act as a starting point for national policy makers, because the goals usually find a social backing at national level, albeit varying degrees. Every goal does not have equal acceptance from every nation, but every nation may find reasonable reception in one way

or another. This help dissemination of the outcomes as the goals usually have reception from different segments of society.

Consequently, international organisations, especially the UN and the EU have active interests in cybersecurity because of the internal pressure coming from their organs to secure their organisational resources and interests and the demands from the member states. The evaluation observes that not only the member states, but also other nations benefitted from alien organisations. This is clear in the EU case that non-member states would make use of the principles, mechanisms, and means produced in Brussels.

Evaluation of cybersecurity indicates explicitly that without taking into account of international organisations/involvements it would be an illusion or misleading conclusion to reach a sound and effective solution to cybersecurity issues. In short, international efforts should be supported by national, regional and local actors as well as international institutions to eradicate cybercrime and promote cybersecurity for the humanity.

References:

Council of Europe, (2026). 'Department for the Execution of Judgments of the European Court of Human Rights', **Country Factsheet of Turkiye**, https://rm.coe.int/turkiye-eng/488029c483, (28.03.2026).

Council of the European Union, (2026a). 'How the EU combats cybercrime', https://www.consilium.europa.eu/en/policies/a-cybersecure-society/, (05.03.2026).

Council of the European Union (2026b). 'Timeline - Cybersecurity', **EU cybersecurity: strategy and key policies**, https://www.consilium.europa.eu/en/policies/cybersecurity/timeline-cybersecurity/ (03.03.2026).

Cyber Resilience Act, (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council, **Official Journal of the European Union**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847 (17.03.2026).

European Commission, (2020). 'The EU's Cybersecurity Strategy for the Digital Decade', **Joint Communication to the European Parliament and the Council**, file:///D:/Downloads/join2020_18_en_act_part1_v9_-_copy_2DD42D12-B246-B9BE-E927D92051AE4753_72164.pdf (15.03.2026).

European Cyber Security Organisation -ECSO, (2026). https://ecs-org.eu/ (15.03.2026).

European Union Agency for Cybersecurity - ENISA, (2019). ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification

and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881 (13.03.2026).

European Union Agency for Cybersecurity -ENISA, (2026). https://www.enisa.europa.eu/ (14.03.2026).

G. Dede, A. M. Petsa, S. Kavalaris, E. Serrelis, S. Evangelatos and I. Oikonomidis, (2024). "Cybersecurity as a Contributor to United Nations SDGs towards enhancing the ESG Reporting," **2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE),** Chania, Greece, pp. 1-6, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10654435 (10.03.2026).

Ige, A.B. Kupa, E. & Ilori, O. (2024). 'Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future', **GSC Advanced Research and Reviews**, 19(03), 344–360.

Kutlu, Ö. (2025). 'The Weaknesses of the International System in Keeping and Maintaining the Global Order', (in Eds. Bulut, M. & Korkut, C.) **Sustainable Economy and Finance in the Age of Global Transformation: Governance, Policies and Technologies**, Ankara: Turkish Academy of Sciences, pp. 35-70, (in Turkish).

Mandal, S. (2024). 'Cybercrime Classification: A Victimology-Based Approach', **Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024**, University of Johannesburg, https://papers.academic-conferences.org/index.php/iccws/issue/view/30/33 (16.03.206).

OCSC, (2022). **Cybersecurity and Sustainable Development: An Intersectional Analysis**, https://ocsc.com.au/wp-content/uploads/2022/08/Cyber-Security-and-Sustainable-Development-2022.pdf, (12.03.2026).

Rupp, C. (2026). 'The UN's New Global Mechanism on Cybersecurity', **Interface**, https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity (10.03.2026).

Sachs, A. Schmalfeldt, I. & Zettl-Schabatt, K. (2024). 'The EU's Application of the Cyber Diplomacy Toolbox', Research Paper 2, February, **European Repository of Cyber Incidents**, https://eurepoc.eu/publication/right-thoughts-right-words-right-actions-the-eus-application-of-the-cyber-diplomacy-toolbox/ (12.03.2026).

UNDP, (2026). 'Background on the Goals', **Sustainable Development Goals**, https://www.undp.org/sdg-accelerator/background-goals (05.03.2026)

UNICEF, (2024). 'Violence against children widespread, affecting millions globally', https://www.unicef.org/press-releases/fast-facts-violence-against-children-widespread-affecting-millions-globally, (12.03.2026).

United Nations General Assembly, (2024). 'United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes', **Resolution adopted by the General Assembly on 24 December 2024**, https://docs.un.org/en/a/res/79/243. (01.03.2026).

United Nations Tourism, (2026). "International tourist arrivals up 4% in 2025 reflecting strong travel demand around the world", https://www.untourism.int/news/international-tourist-arrivals-up-4-in-2025-reflecting-strong-travel-demand-around-the-world?utm_source=chatgpt.com (12.03.2026).

United Nations, (2021). 'Cybersecurity in the United Nations system organizations', **Report of the Joint Inspection Unit,** https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf (12.03.2026).

United Nations, (2026a). **Millenium Development Goals**, https://www.un.org/millenniumgoals/ (03.03.2026)

United Nations, (2026b). 'Sustainable Development Goals', **Department of Economic and Social Affairs**, https://sdgs.un.org/goals (01.03.2016).

United Nations, (2026c). 'Guide to Developing a National Cybersecurity Strategy', Third Edition, https://www.un.org/counterterrorism/sites/default/files/2026-01/2025-ncs-guide.pdf, (12.03.2026).