Role of International Organisations in Cyber Law Harmonisation and Human Rights Protection

Sameer Haider*

Abstract

The harmonisation of cyber laws proves to be rather difficult as each country has varying approaches to human rights protection, varying institutional capacity, and different national legal systems. This research identifies the work done by international organisations (IOs), specifically by the United Nations, the European Union and the Council of Europe, in developing common legal standards for cybersecurity, combating cybercrime, and safeguarding digital rights. The research adopts a qualitative doctrinal approach, in which the contents of the international legal documents, as well as the various active institutional mechanisms and decisions of international courts and tribunals, are comparatively analysed, taking into account the Budapest Convention, GDPR, and new international frameworks. The analysis finds that international organisations enable legal convergence to occur in both binding treaties and non-binding standards, technical cooperation and institutional coordination. State sovereignty, changing national practices, weaknesses in institutional powers and conflicts between security and fundamental rights, however, do still limit harmonisation. This paper further establishes that the use of common legal instruments is not always enough to guarantee effective implementation or similar protection of human rights at the national level. It argues that the push for meaningful harmonisation in cyber law is more about the coordinated implementation of law, the institutional capacity-building and effective human-rights safeguards rather than legislative harmonisation alone. These findings contribute to understanding the relationship between international legal cooperation, domestic enforcement, and human rights protection in global cyber governance.

* Lawyer, Junior Partner, Israr Law Associates, Director, Child Protection at FIKER, Gilgit-Baltistan, Pakistan; email: sameerofficial309@gmail.com
Article History: Received: 05-05-2025; Received in revised form: 28-09-2026; Accepted: 05-10-2026.
Available online: 26-10-2026
DOI: https://doi.org/10.24312/ucp-jlle.04.01.535
CC BY OPEN ACCESS

Keywords: Human Rights, Privacy, Data Security, Cybercrime, Budapest Convention, GDPR.

Introduction

Cyberattacks pose an increasing threat to the integrity of the sectors that are crucial to our social and economic prosperity. A significant increase in cybersecurity threats has been observed in recent years, surpassing society's ability to prevent or adequately respond to them (Doyle, 2022). In the widest sense, the protection of data and digital networks from errors, attacks and hacking is called cybersecurity. Comprising various policies and a wide variety of practices, it is aimed at safeguarding data and sustaining the confidentiality, availability and integrity of digital resources (von Solms & van Niekerk, 2013). Significant harm to organisations, individuals, and even entire countries can be caused by cyber threats such as malware, data breaches and many others. These evolving threats indicate the necessity of harmonised international regulations to address cybersecurity challenges while safeguarding fundamental human rights (Singh, 2023).

Cybercrime refers to the illegal activities carried out by means of Information and Communications Technology (ICT) tools; these instruments are used both to commit crime and to target crime (AllahRakha, 2024). Hacking, illegal interception of telecommunications, cyberstalking, identity theft and misrepresentation are foremost examples of cybercrime. Both people and nation-states are capable of committing these crimes. They cause serious problems to the availability, confidentiality, integrity, and security of vital computer infrastructure, which may lead to unnecessary costs, financial loss, reputational harm, interruption of corporate operations, and loss of intellectual property (Broadhurst, 2006; Gordon & Ford, 2006). Cybercrimes are rapidly increasing at an alarming rate globally (Lallie et al., 2021).

The growth of numerous cybercrimes globally is due to the absence of effective legislation and tools to punish and prosecute the perpetrators (Gastorn, 2017). Despite the efforts of international organisations, the harmonisation of cyber laws remains a principal challenge due to the transnational nature of cyberspace and the lack of codified global norms (Brenner & Koops, 2004; Clough, 2014). These enable cybercriminals to exploit the regulatory differences,

raising concerns about the protection of civil liberties and causing irregularities in legal structures (Broadhurst, 2006; Tropina, 2024). The hurdles these organisations face in balancing human rights with security needs are mostly neglected by the existing research. It is necessary to research these obstacles, as they highlight the need for a deeper investigation into their role and effectiveness.

Several international organisations such as the United Nations (UN), the Council of Europe (CoE) and the European Union (EU) have been making efforts in shaping legal frameworks and harmonising legal and institutional responses. For example, the Budapest Convention is the first international agreement established by the Council of Europe to combat cybercrime by harmonising national laws and promoting cooperation while emphasising the significance of human rights (AllahRakha, 2024). It mainly focuses on creating a framework to encourage cross-border cooperation between law enforcement authorities and harmonising cyber laws (Nguyen & Golman, 2021). Similarly, the European Union's General Data Protection Regulation (GDPR) has become a benchmark in protecting individual privacy and giving them more control of their data (Blind et al., 2023). Through the United Nations Office on Drugs and Crime (UNODC), the United Nations (UN) is also working to prevent cybercrimes (UNODC, n.d.-a). The UNODC Global Programme on Cybercrime offers technical guidelines that promote international collaboration, raise awareness of cyber threats, and enhance capacity, with a main focus on developing countries (Billow, 2023; UNODC, n.d.-a). The UNODC cybercrime repository operates as a primary data tool for global cybercrime control (UNODC, n.d.-b).

While numerous international organisations have taken significant initiatives to combat cybercrime and promote cybersecurity, the existing studies focus on their achievements, giving less attention to the challenges they face in harmonising global cyber regulations and protecting fundamental human rights. Besides the Council of Europe's Budapest Convention on Cybercrime and the African Union's Convention on Cyber Security and Personal Data Protection, the progress in incorporating cyber rules into international law has been relatively limited (Novas-Pena, 2024). Furthermore, limited attention has been given to how the balance between the execution of cybersecurity measures and the protection of human rights such as freedom of expression and

privacy is managed by the international organisations (Allahrakha, 2023).

This research seeks to address how international organisations help with the harmonisation of cyber law and the protection of human rights, and how do state sovereignty, legal fragmentation, institutional differences and challenges of enforcement influence the implementation and effectiveness of international cyber governance structures?

The objective of this paper is to critically analyse the legal and institutional role of international organisations, to map the shortcomings of prevailing harmonisation options and suggest approaches to enhance international cooperation while protecting core human rights in cyberspace.

Research Methodology

This study employs a qualitative doctrinal research methodology, supported by comparative and thematic legal analysis, to examine the contribution of international organisations to cyber law harmonisation and human rights protection. It draws upon primary legal sources such as international conventions, government regulations, institutional documents and judicial decisions, in addition to scholarly academic writing.

The study adopts the deductive proposition that international legal harmonisation requires more than the formal adoption of common standards; it needs to be backed by implementation mechanisms, cooperation of institutions, the capability to enforce and protection of fundamental rights in these countries. The selected international frameworks are given a critical analysis using this proposition as an analytical basis.

The selection of sources was based on the four criteria: relevance to the research question, legal authority, institutional significance, and relevance to cybersecurity, international cooperation and human rights. For all these reasons, the focus of the analysis is on the United Nations, Council of Europe, European Union, and certain regional and international organisations.

The chosen instruments and judicial acts are analysed in relation to four criteria: the nature of their legal obligations, the way they seek to facilitate international cooperation, implementation and enforcement provisions and protection of fundamental rights.

Comparative analysis identifies similarities and differences between binding and non-binding instruments, and thematic analysis looks at frequent issues related to sovereignty, jurisdiction, institutional capacity, and the balance between security and individual rights.

The research is done as a doctrinal study, and it does not rely on original statistical or other field data to assess the effectiveness of the legal/institutional setup. Its findings therefore concern the legal design, implementation limitations, and normative implications of the frameworks examined.

Literature Review

Existing scholarship identifies the transnational nature of cybercrime and the fragmentation of national legal systems as major obstacles to effective international cybersecurity governance. Singh (2023) references a connection between the changing nature of cyber threats and fundamental rights, focusing on how these intersections impact laws and policies, and Bardhan and Singh (2023) propose that international organisations help to decrease legislative differences. These studies set the agenda for comparable laws and conventions, but offer a more limited analysis of the actual functions of international conventions or frameworks in diverse institutional and jurisdictional contexts.

A central issue in international legal harmonisation concerns the distinction between binding legal obligations and voluntary regulatory standards. Abbott and Snidal (2000) describe various benefits of hard and soft law as a form of international governance, including legal certainty, flexibility, cooperation and state sovereignty. The difference is of particular importance to cyber governance, where binding agreements like the Budapest Convention coexist with non-binding guidelines and cooperative arrangements. These mechanisms can promote regulatory convergence, but may be less effective given differences in domestic implementation and enforcement of these regulations.

The theoretical foundations of cyber law harmonisation can also be understood through state sovereignty, legal fragmentation, and functionalist approaches to international cooperation. State sovereignty provides a reason for governments to have discretion over the adoption and enforcement of international cybersecurity standards, whether present or missing (Efrony & Shany, 2018;

Daskal, 2015). Legal fragmentation draws attention to the challenges caused by the overlapping regulatory regimes, conflicting claims to jurisdiction and diverse domestic requirements (Koskenniemi & Leino, 2002; Brenner & Koops, 2004). Functionalist explanations, on the other hand, focus on providing an account of how international organisations promote cooperation by solving technical and legal issues that are too difficult for states to resolve on their own (Mitrany, 1948; Abbott & Snidal, 1998). Considered alongside Abbott and Snidal's (2000) distinction between hard and soft law, these views make it evident that harmonisation is more about the convergence of different institutional interests, different national regulatory powers and different implementation capacities than about the creation of common rules. The theoretical guidance underpinning the study is based on the comparative evaluation of international organisations and how they contribute to legal convergence and protection of human rights (Abbott & Snidal, 1998, 2000; Tropina, 2024).

The relationship between cybersecurity and human rights constitutes another important dimension of the literature. Tropina (2024) critically examines the human-rights implications of the United Nations cybercrime treaty negotiations and emphasises the significance of proper safeguards in international criminal cooperation. However, as her analysis clearly shows, more powers to investigators and more international cooperation do not always mean rights protection. This is especially significant when there are differences between domestic and international legal systems and oversight mechanisms affect the application of international standards. Evaluating the effectiveness of cyber law harmonisation therefore needs to go beyond the contribution to security cooperation and needs to take into account its capacity to preserve fundamental rights.

The topic of the relationship between cybercrime law and human rights has further been exposed in recent developments in the international arena. The United Nations Convention against Cybercrime (2024) is an attempt to adopt a broader approach to international cooperation, and the Council of Europe's Framework Convention on Artificial Intelligence (2024) brings new developments in AI into the focus of international regulation and its consequences for human rights, democracy and the rule of law.

However, the institutional, normative and enforcement aspects of cyber law harmonisation are not sufficiently combined in the existing scholarship to yield a comprehensive comparative study. This research looks at that problem because it questions how international organisations can be part of these efforts towards legal convergence and the impact common standards might have in practical implementation depending on domestic implementation, institutional capacity and safeguards for human rights.

Existing research has examined the contributions of international organisations to cybersecurity cooperation, cybercrime regulation, and digital rights protection. However, comparatively limited attention has been given to the relationship between international legal harmonisation, domestic implementation, and the effectiveness of human-rights safeguards across different institutional frameworks.

Although instruments such as the Budapest Convention and GDPR are frequently discussed, their contributions are often assessed independently rather than through a comparative examination of their legal obligations, enforcement arrangements, and practical limitations. Moreover, the growing importance of emerging technologies and recent international legal developments requires renewed consideration of how international cooperation can be strengthened without undermining fundamental rights.

This study addresses these gaps through a comparative doctrinal assessment of selected international organisations, legal instruments, and judicial decisions, focusing on the distinction between formal regulatory convergence and effective, rights-based implementation.

International Organisations in Harmonising Cyber Law and Protecting Human Rights

Cybercrime legislation holds significant importance in this era where cyber threats are growing at an alarming rate as technology continues to advance and control many aspects of our daily life. To counter this menace, numerous international organisations have been contributing to establishing legal frameworks, fostering international cooperation and resolving challenges raised by cyber threats, while protecting human rights (Barber & Kumar, 2024). Harmonised legal mechanisms are

essential to create consistency and enforceability across jurisdictions due to the transnational nature of cybercrimes and digital rights violations.

The role of some key Regional, multinational, and Global Organisations in the harmonisation of cyber laws and human rights protection is discussed below:

Council of Europe (CoE)

CoE is a European human rights organisation, established in 1949, consisting of 46 members that actively work together to promote equality, democracy, freedom of expression, and protect fundamental human rights (Council of Europe, 1949). In creating frameworks that guide national policies on cybercrime and human rights in cyberspace, CoE has played a significant role as one of the main regional organisations. Cybercrime Programme Office of the Council of Europe (C-PROC), affiliated with CoE, helps countries globally in combating the hazards of cybercrime. The basis of its regulation is the Budapest Convention, which is a major international treaty on cybercrime (Neethu, 2020).

The Budapest Convention, opened for signature on November 23, 2001, was the first-ever international treaty and a collective action by member and some non-member states of the Council of Europe against cybercrime. This convention ensures respect for human rights and has a critical impact on international anti-cybercrime legislation (Nguyen & Golman, 2021), with a prime goal of developing effective mechanisms for international cooperation on cybercrime legislation by harmonising domestic criminal laws in specific areas (Rossini & Green, 2015). Regardless of its regional (European) nature, this treaty became the most effective tool for the international protection of all institutions that use computer technologies. This resulted in the adoption of this agreement by a number of states in their legal systems, treating it as a role model, which are neither parties to the Convention on Cybercrime nor members of the Council of Europe (Milik, 2019).

Another development is the ‘Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law' adopted in May 2024, opened for signature in September 2024. It creates an international treaty framework focused on the impact of artificial intelligence on human

rights, the freedom of democratic elections and the rule of law. It shows the Council of Europe's changing perspective on the new digital technologies, as it places great value on transparency, accountability, risk assessment and effective remedies. However, it is important that states ratify the Convention and ensure that the principles in the Convention are applied on the ground through positive, concrete domestic regulatory acts in order to contribute to international harmonisation (Council of Europe, 2024).

Although the Budapest Convention makes a significant contribution to the process of harmonisation of cyber law, it does not create complete uniformity among national legal systems (Clough, 2014). Its effectiveness is dependent on the willingness of participating and adopting states to integrate its standards into their own laws and have the institutional mechanisms for implementation (Nguyen & Golman, 2021; Wicki-Birchler, 2020). The Convention is thus an important instrument towards legal convergence and international cooperation, but the fact remains that certain differences in domestic legislation and enforcement impede the extent of harmonisation that is realistic in practice.

Interpol

International Criminal Police Organisation, commonly known as Interpol, is an international law-enforcement organisation that promotes international police cooperation to combat crime with 197 member countries (Billow, 2023) and protect the rights of individuals (Calcara, 2020). Interpol increased the scope of its work to both legal harmonisation and law enforcement by identifying gaps between the legal structure and criminal phenomena (Billow, 2023; Calcara, 2020). Interpol carried out significant initiatives to prevent cybercrime and put effort into law enforcement on cybercrime as well (Li, 2007).

Interpol’s secure communications network (I-24/7) is an advanced instrument that enables cross-border information and intelligence sharing, required in cybercrime investigations (Peters & Jordan, 2019). Domestic police forces and verified users obtain instant access to the organisation’s database with the help of this system (Calcara, 2020).

Interpol's role at the enforcement and cooperation levels is especially important, but the strength of its influence is subject to

the capacities of the institutional structures and legal powers of the member states. The mere existence of international police co-operation does not cure the differences between national criminal laws, evidentiary requirements or procedural safeguards (Brown, 2015; Calcara, 2020). Interpol thus facilitates operational cooperation among law enforcement authorities but cannot independently harmonise national cybercrime legislation.

United Nations (UN)

The UN is one of the most remarkable and powerful international organisations in the world that intends to safeguard common freedoms, provide security, maintain harmony and encourage partnership among its 193 member states (Neethu, 2020).

Through the United Nations Office on Drugs and Crime (UNODC), the UN is actively engaged in combating cybercrime and assists countries in developing cybercrime legislation aligned with international standards. The UNODC Global Programme on Cybercrime offers technical support in international collaboration, capacity building and prevention and awareness-raising, particularly in developing countries (Neethu, 2020).

The United Nations Convention against Cybercrime, adopted by the General Assembly on 24 December 2024, represents an important development in global cybercrime governance. It outlines steps for co-operation to tackle the identified cybercrimes and to exchange electronic evidence in crime investigations. In contrast to the Budapest Convention, which originated from a regional negotiation process, the UN instrument has been developed through an international negotiation process in a global manner. Its effectiveness will, however, depend on ratification, domestic implementation, and adequate human-rights and procedural safeguards. This greater global reach invites, however, the potential for the convergence of laws, as well as privacy and other fundamental rights concerns in a cross-border investigation (United Nations General Assembly, 2024).

The International Telecommunication Union (ITU) promotes international cooperation through its Global Cybersecurity Agenda in cybersecurity, including capacity building and technical assistance (AllahRakha, 2024).

United Nations' Open-ended Working Group (OEWG) ensures cooperation by creating a legal framework for international cybersecurity. It addresses new ways to foster international collaboration on cybersecurity issues by reviewing and developing suggestions regarding the application of international law in cyberspace (Bardhan & Singh, 2023).

One of the main advantages of the United Nations is its ability to reach out to a multitude of states, which have, of course, diverse legal frameworks and political agendas, and converge around the common issues of cybersecurity and the potential ways and means to solve them (Tropina, 2024). But the variety of country interests compounded this, as well, in lessening the ability of these initiatives to bring consistency and enforceability to domestic cyber laws. In fact, UN involvement in building international consensus and cooperation is important, so the implementation is mainly left to individual states.

Organisation for Economic Cooperation and Development (OECD)

OECD, established in 1961 and consisting of 38 member economies, is a multinational organisation that contributes to promoting frameworks to combat cybercrime and strives for the improvement of the quality of life of its citizens (OECD, 1960; OECD, n.d.). To ensure Information and Communication Technology (ICT) infrastructure and secure communication methods, it encourages its members to develop an internationally coordinated approach (OECD, 2002). To address concerns like cryptography, privacy and data protection, it creates agreements between countries (Neethu, 2020).

The OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (1980) laid out a key framework for international data privacy laws, ensuring people's right to privacy. Instead of protection against surveillance, it focuses on the processing, dissemination and collection of information for global data transfers (Ünver & Kim, 2022).

The OECD also provides a Cybersecurity Policy Framework that guides its members in building coherent and effective cybersecurity legislation. It also highlights how essential risk

management, international cooperation and public-private partnerships are to enhance cybersecurity (Bardhan & Singh, 2023).

The OECD model shows the value of creating shared principles and policy parameters without having to be the same at the national level. There is, however, a need for coordinated standards to be implemented in a variety of ways across different jurisdictions. This role is more effective in driving policy convergence and interoperability than uniformity and enforceable cybercrime laws.

European Union (EU)

The EU has adopted significant frameworks and policies in combating cybercrime by enacting legal harmonisation policies and coordinated law enforcement while focusing on civil liberties in the anti-cybercrime field (Li, 2007).

The General Data Protection Regulation (GDPR), adopted in 2016 and applicable from May 2018, is a comprehensive data protection framework (Wicki-Birchler, 2020), which sets global standards for data protection, establishes strict requirements for data processing, grants people greater authority over their personal information and enforces sanctions for failure to comply. The influence of data protection laws has encouraged many European countries to synchronise their laws in accordance with the GDPR regulations to foster international trade and data exchange (Bardhan & Singh, 2023).

European Union Agency for Cybersecurity (ENISA) is an EU body dedicated to fostering the process of combating cybercrime in European countries by assisting its members to be well prepared to detect and prevent ongoing threats (European Union Agency for Cybersecurity [ENISA], n.d.). It aims to develop mutual understanding of the key roles, skills, competencies and knowledge by establishing the European cybersecurity skills framework (AlDaajeh et al., 2022).

The Court of Justice of the European Union (CJEU) also plays a crucial role in ensuring that EU digital regulations align with fundamental rights under the EU Charter of Fundamental Rights. It has made judgments in cases connected with government surveillance, automated decision-making, and information retention guidelines (Granger & Irion, 2014). The EU's commitment to

privacy was strengthened when the Tele2 Sverige AB ruling (2016) struck down indiscriminate data retention legislation (Bendiek & Maat, 2019).

There exists a relatively high level of regional legal harmonisation in the EU as there are common institutions and legal mechanisms in place to support the regulatory framework. But this is mainly a regional type of model, and it does not address the conflict between EU and non-EU jurisdictions sufficiently on its own. Furthermore, the efficacy of EU cybersecurity and data-protection legislation is contingent on even and continuous application and enforcement in the EU Member States. The EU is therefore a good example of the benefits of increased regional integration and of the ongoing challenges of getting regional harmonisation onto a global level.

Asia-Pacific Economic Cooperation (APEC)

APEC is a regional economic forum that was established in 1989. With 21 member economies, it encourages free trade within the Asia-Pacific region and enhances economic growth and prosperity (Waters, 2009). APEC took significant steps to encourage cooperation and information sharing across borders about potential risks to combat terrorism (Neethu, 2020).

APEC Cross-Border Privacy Rules (CBPR) system was established in 2011 as a voluntary cross-border personal data protection framework while facilitating cross-border data flows. Normally, the system allows participating businesses to certify that they exchange data in accordance with privacy requirements, without unnecessarily restricting cross-border data transfers (Raul, 2021).

The APEC Privacy Framework, endorsed in 2004, with implementation guidance added in 2005 by APEC, aims to assist the development of data privacy protection with its guiding principles in such a way that enhances the free flow of information for economic development in the Asia-Pacific region (Waters, 2009; Greenleaf, 2009). The main objective of its guiding principles is data protection and privacy, and balancing individual rights with the growth of the economy while giving direction for their implementation at the domestic and international levels (Raul, 2021).

APEC's work demonstrates the benefits of flexibility in the process of establishing privacy and cybersecurity requirements in jurisdictions with different legal and economic systems (Waters, 2009; Greenleaf, 2009). This flexibility, however, also imposes some constraints, as cooperative and voluntary solutions can only achieve a certain level of uniformity that may be insufficient to those of legislation. The interoperability and regional cooperation aspect of APEC is limited, however, in its power to make broad and binding harmony (Greenleaf, 2009).

African Union (AU)

The African Union (AU), established in 2001, is an intergovernmental regional entity with 55 sovereign African States that aims to accelerate political and socio-economic integration and unites sovereign states throughout the whole African continent to foster economic development and coordination for the progressive achievement of the Union's goals by harmonising the regulations between the present and future regional economic communities (Orji, 2018).

AU established the African Union (AU) Convention on Cyber Security and Personal Data Protection in 2014, as the rise of information technology and the penetration of the internet indicated the need for effective legislation for cybersecurity in African communities (Orji, 2018). This convention, also known as the Malabo Convention, acts as an essential instrument in combating cybercrime and safeguarding personal data in Africa, addressing concerns like cybersecurity, internet commerce, and digital rights (AllahRakha, 2024).

The African Commission on Human and Peoples' Rights (ACHPR) adopts resolutions to address various issues related to human rights and promotes regional cooperation in fighting cyber threats. It plays a pivotal role in the protection and promotion of human rights across Africa (Mavenjina, 2018). Likewise, the African Commission on Human and Peoples' Rights (ACHPR, 2019) underlines the significance of online freedom of speech and defence against governmental surveillance (Masters, 2022).

The African Union framework represents an important attempt to align the cybersecurity, data protection and human-rights approaches. However, some limitations exist due to the various legal

frameworks and capacities across the countries, which can impact the uniform application of regional standards (Orji, 2018; Abdulrauf & Fombad, 2016). It is therefore the Convention that is helping to achieve the convergence of regional law, but the effectiveness of this depends on available implementation in domestic law.

Comparative Assessment of Institutional Approaches

Comparative analysis shows that there is no single/cross-sectoral approach to international co-operation regarding cyber law harmonisation, but rather different approaches in the form of law and institutions. Cooperation based on a treaty is proposed by the Council of Europe (Budapest Convention) and supported by the European Union (EU) via binding regulatory instruments like the GDPR. Interpol, on the other hand, facilitates operational coordination between the individual law enforcement agencies, while the United Nations is a more comprehensive forum for multilateral cooperation. The OECD and APEC rely substantially on voluntary standards and policy cooperation, while the African Union promotes regional legal convergence through the Malabo Convention.

The design of the institutions serving as a vehicle for harmonisation is seen to have a significant impact on harmonisation processes, as shown by these differences. Binding instruments can create more enforceable legal commitments, and the ways this is done will depend on a state's legislative and institutional structures. Voluntary frameworks, on the other hand, may offer more flexible approaches to measuring compliance, and can work well alongside a variety of domestic laws as long as they are maintained. Effective cooperation, such as with INTERPOL, in the operational aspect of criminal investigations will help expand the use of cross-border investigations without necessarily having to be applied to address substantive differences between national cybercrime legislation.

Thus, the effectiveness of international organisations goes beyond a mere count of the number of frameworks or initiatives being put in place. But their contribution should be measured not only in terms of the implementation at the domestic level, institutional capabilities underpinned by enforcement, but also the incorporation of fundamental rights safeguards. The analysis concludes that the best way to establish convergence at the

international level is to have stepped-up coordination and accountability for the adoption of common international standards, rather than formal harmonisation.

Case Law Illustrating the Intersection of Cybersecurity and Human Rights

Tele2 Sverige AB v. Post-och telestyrelsen (2016) (C-203/15)

In this case, the Court of Justice of the European Union considered national retention laws which were in force at the time, requiring the "general and indiscriminate" retention of location data and traffic data associated with electronic communications. The Court went on to find that EU law did not allow for such blanket retention for law enforcement purposes and stressed the need to ensure that there were still strict limitations and safeguards for interference with fundamental rights. The judgment relied on Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, reaffirming the importance of privacy and personal data protection.

The ruling shows the importance of not allowing the collection and retention of communications data to be unlimited in the name of public security. Perhaps more broadly, its importance for cyber law harmonisation is in clarifying the need for consistency of common investigative and security measures which should be consistent with the basic rights and proportionality requirements.

Digital Rights Ireland Ltd v. Minister for Communications (2014)

The Court of Justice of the European Union in this case struck down Directive 2006/24/EC, which called for the retention of some electronic communications data. The Court determined that the Directive disproportionately violates the fundamental human rights to privacy and protection of personal data, since there were broad retention obligations lacking limits and safeguards.

It is worth noting in the judgment that the existence of a ‘regional harmonisation process' is not enough to conclude that there is ‘regional competence' in this field. A second key element of substantive compatibility is that those obligations are not in contradiction with fundamental rights. In line with Tele2, the

decision holds that notions of necessity, proportionality, and effective legal safeguards should be integrated into robust cybersecurity and investigative policies and mechanisms to make security goals more than just an overriding concern.

Big Brother Watch and Others v. United Kingdom (2021)

In this case, the European Court of Human Rights has addressed surveillance and bulk interception under the European Convention on Human Rights. The Grand Chamber ruled that the United Kingdom's surveillance laws infringed upon Article 8 concerning privacy and Article 10 concerning freedom of expression.

The judgment highlights the need for effective oversight over surveillance measures and sufficient independent control and protection against arbitrary interference. What is relevant for international cyber governance is that despite a focus on security cooperation and technological surveillance capacities, there is a need for effective and enforceable procedures that provide protections. Unlike instruments primarily concerned with facilitating criminal investigations, human-rights jurisprudence provides substantive standards against which the legality of surveillance arrangements can be assessed.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

In this case, the Supreme Court of India recognised privacy as a fundamental right protected under Article 21 and other provisions of Part III of the Constitution. The judgment connected privacy with personal dignity, liberty and autonomy, establishing an important constitutional foundation for evaluating state interference with personal information.

The decision, which was not directly about international harmonisation of cybercrime, is nonetheless of use for giving a non-European insight into the protection of digital rights in the domestic sphere. It illustrates how international cyber security standards are part of different constitutional systems, and the importance of maintaining compatibility in their application with domestic constitutional guarantees to fundamental rights. It thus bolsters the position that preserving domestic constitutional protection, rather

than just copying and pasting the same laws, is a way of converging on international law.

Comparative Jurisprudential Findings

These decisions collectively show that there has to be more consideration of meaningful protection for substantive rights in the field of cybersecurity and digital governance than just uniformity of regulation. The CJEU rulings introduce limits on indiscriminate data retention, the European Court of Human Rights stresses the importance of protecting privacy from surveillance, and a key Indian Supreme Court decision lays down the constitutional basis for privacy protection beyond Europe. Decisions demonstrate the importance of the concepts of legality, necessity, proportionality and accountability. But international law harmonisation must not only encourage state collaboration but also recognise minimum standards for state action to protect individuals from undue infringement on their fundamental rights.

Challenges and Normative Tensions in Global Cyber Governance

In spite of the efforts of international organisations, cyber law harmonisation is still hampered by the lack of convergence in regard to the national legal systems, the scope of the authority, the capacity of their institutions and their foundational rights approaches (Clough, 2014; Nguyen & Golman, 2021). The problems illustrate that the implementation of common international standards will not lead to this automatically being the same at the national level or in terms of the enforcement of these standards across countries.

Jurisdictional Conflicts and State Sovereignty

The constantly evolving threat landscape of cybercrime helps to explain the jurisdictional challenges, as criminal activity, the underlying infrastructure, affected evidence, and individuals can be in various states. This may then lead to "national claims" of jurisdiction by national authorities, and difficulties in the investigation and prosecution of crimes related to weaknesses in criminal law. Lack of cooperation between domestic law on crime

and effective responses to transnational crime is highlighted in the 'Love Bug' incident of 2000 (Brenner & Koops, 2004).

The myriad of challenges also highlights the fact that global harmonisation is in tension with the principle of state sovereignty. Although there are international agreements that require states to have shared responsibilities and joint mechanisms for tackling crime, states have a significant degree of authority in relation to the exercise of criminal jurisdiction and criminal enforcement. Thus, there will be no jurisdictional conflict-free convergence under international law without effective mechanisms for mutual legal assistance and cooperation.

Differences in National Legislation and Enforcement Capacity

There are significant variances in definitions of offences, investigation, the use of privacy safeguards and enforcement in national cyber laws (Clough, 2014; Gordon & Ford, 2006; Brown, 2015). These differences can allow cybercrime operations to take place in jurisdictions where the laws are less sophisticated, and make it more difficult to gather evidence and prosecute out-of-jurisdiction perpetrators of crimes (Lessig, 2006).

In developing countries, having limited financial and technical resources and digital forensic capabilities may pose challenges in implementing international standards, thus making the problem even more important (Billow, 2023; Broadhurst, 2006; Brown, 2015). As a result, having adopted harmonised legislation, outcomes of enforcement cannot be assumed to be equivalent. Besides legal standard-setting, international organisations therefore need to reinforce it with technical and capacity-building assistance along with institutional development.

Cybersecurity and Fundamental Human Rights

The interaction of cybersecurity and human rights involves an ongoing normative struggle. The use of electronic surveillance, intercepting information, obtaining personal data and sharing it can serve very legitimate security goals, but also invade the privacy and expression rights of individuals (Tropina, 2024).

This reveals that cybersecurity measures must meet the necessity, effective oversight and legality requirements, as well as proportionality. International harmonisation should, therefore, go

beyond the common investigative powers to provide for enforceable and binding procedural safeguards and remedies. If not, a convergence of laws could enable a multi-territorial approach to cooperation, but also raise the possibility of such an outcome as to risk of disproportionate interference with fundamental rights.

Cross-Border Cooperation and Legal Fragmentation

Especially in international investigations, electronic evidence sources are often outside the investigating jurisdiction (Daskal, 2015; Brown, 2015; Spiezia, 2022). The domestic procedures, mutual legal assistance arrangements and data protection obligations of each nation must be considered, which have the potential to delay access to evidence and hinder cooperation (Peters & Jordan, 2019).

Instruments like the Budapest Convention set out the guidelines for international collaboration, but their applications and impacts depend on the participation, implementation and institutional coordination at the national level. More international frameworks could emerge to allow for more cooperation and coordination, but at the same time prevent law-mix-up and different legal interpretations. This shows that harmonisation should consider compatibility between the different legal regimes, but does not necessarily mean the proliferation of international instruments.

Emerging Technologies and Public–Private Regulation

The use of advanced and evolving digital technologies, such as Artificial Intelligence and blockchain, poses questions and challenges to traditional principles of responsibility, accountability and jurisdiction. Whatever regulatory reaction they have to make must consequently be flexible, but also offer enough predictability and legal protection for human rights (Scherer, 2016).

Moreover, private tech companies are taking over digital infrastructure and a large percentage of personal data, as well as communication services (DeNardis & Hackl, 2015; Klonick, 2018). While there are regulatory standards set at the state and international level, it is not always clear how well these regulations are being put into practice (Klonick, 2018); it seems cooperation with these private actors is essential. Good governance for the cyber domain, therefore, should include clear accountability, a regulatory

framework and processes for the increased participation of the public and private sector in a consistent manner with fundamental rights.

Analytical Synthesis

These challenges reveal the interconnections of governance dilemmas between sovereignty and harmonisation, security and human rights, developed and developing states and public and private governance authorities. Consequently, the other way to mitigate legal fragmentation is for international organisations to establish common standards, which will crucially rely on domestic follow-up and implementation, institutional cooperation, a level playing field in terms of capacity-building, and the establishment of enforceable protection mechanisms. Different initiatives, therefore, are needed within a legal framework and institutional dimension for meaningful harmonisation beyond legislation.

Suggestions and Recommendations

The following are some suggestions and recommendations for international organisations to enhance cybersecurity measures globally:

(a) International organisations should facilitate expanded involvement in current cybercrime cooperation efforts, such as the United Nations Convention against Cybercrime, and ensure its implementation at the national level; and also ensure proper human rights protection measures. To minimise legislative differences and increase international cooperation on diverse issues without duplicating existing treaty mechanisms, better coordination among the United Nations, the Council of Europe and regional institutions could be offered.

(b) International organisations should further strengthen cross-border electronic evidence-sharing and mutual legal assistance mechanisms, especially by the implementation of the relevant cybercrime conventions. When it comes to cooperation, timely responses, clear and streamlined procedural requirements, judicial oversight, protecting the right to data protection, and guarding against

disproportionate interference with fundamental rights should be given priority.

(c) To enable collaborative investigations in cybercrime and real-time intelligence sharing, organisations like Interpol and the African Union (AU) must improve their cybersecurity department. It is essential to foster cooperation among regional agencies such as the European Union (EU) and the African Union (AU) to harmonise cybersecurity regulations across various economic sectors. The creation of regional cybersecurity centres may also assist in adapting cyber law enforcement measures to address particular regional issues.

(d) The enforcement agencies must ensure that cyber laws and regulations do not violate fundamental rights such as freedom of speech and privacy, etc. It is important to maintain a balance between cybersecurity measures and human rights. There should be strict transparency and oversight mechanisms to avoid the exploitation of surveillance laws. By creating a United Nations Digital Rights Charter, people can be protected from unwarranted data-collecting methods and mass surveillance, as it provides strong principles to safeguard human rights. Furthermore, government surveillance programmes must be supervised by autonomous oversight organisations to maintain accountability in cyber investigations.

(e) Due to insufficient digital forensic capability, inadequate knowledge and resources in technology, law enforcement entities face obstacles in the attribution of cybercrime, forensic investigations and evidence collection. By developing cross-border forensic evidence-sharing platforms, organisations can collaborate in real time while respecting human rights and privacy regulations. Moreover, essential tools required to manage digital evidence and effectively prosecute hackers can be provided to judges, lawyers and law enforcement officers by funding cybersecurity capacity-building initiatives. To organise cyber law implementation strategies universally, it is necessary to establish training initiatives, run by entities like the United Nations Institute for Training and Research (UNITAR).

(f) International organisations need to increase cooperation in the regulation of emerging technology, such as AI and blockchain. The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, adopted by the COE, is important for the understanding and development of regulatory approaches based on the principle of respect for rights. It would be valuable in enhancing accountability, transparency and human rights protection in new digital spaces, subject to its entry into force and effective domestic implementation**.**

Conclusion

This study shows international organisations have diverse and complementary legal and institutional ways of influencing the harmonisation of cyber law. Binding treaties, regional regulations, voluntary standards and operational cooperation all contribute to fostering convergence in national measures to address cybercrime and the safeguarding of digital rights. The effectiveness can, however, not be measured by the adoption of common legal instruments.

Three fundamental conditions for meaningful harmonisation can be illustrated through an institutional and jurisprudential approach: Consistency of legal norms, effective implementation in national legislation and enforceable human-rights protection. International frameworks continue to face limitations with regard to their implementation because of differences in national jurisdiction, institutional capacity and the national interests of sovereigns. Moreover, judicial developments convey the principles of keeping cybersecurity efforts in line with legality, necessity, proportionality and accountability.

International cyber governance continues to emerge, such as most recently in the United Nations Convention against Cybercrime and the Framework Convention on Artificial Intelligence of the Council of Europe. These tools, however, need to be evaluated with regard to the supporting arrangements and protection of fundamental rights.

The three key areas identified for the study to be kept focused are coordinated implementation, institutional capacity-building and rights-based oversight, in addition to the harmonisation of aspects of legislation. This would improve international collaboration and

mitigate the unevenness of different countries applying the same security parameters, and the lack of protection of individual rights.

References

Abbott, K. W., & Snidal, D. (1998). Why states act through formal international organizations. Journal of Conflict Resolution, 42(1), 3–32.

Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. International Organization, 54(3), 421–456. https://doi.org/10.1162/002081800551280

Abdulrauf, L. A., & Fombad, C. M. (2016). The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa? Journal of Media Law, 8(1), 67–97. https://doi.org/10.1080/17577632.2016.1183283

African Commission on Human and Peoples' Rights. (2019). Declaration of principles on freedom of expression and access to information in Africa. https://achpr.au.int/en/documents/2019-11-10/declaration-principles-freedom-expression-access-information-2019

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Allahrakha, N. (2023). *Balancing cyber-security and privacy: Legal and ethical considerations in the digital age*. КиберЛенинка. https://cyberleninka.ru/article/n/balancing-cyber-security-and-privacy-legal-and-ethical-considerations-in-the-digital-age

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure Policy and Development*, *8*(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007

Barber, I. A., & Kumar, S. (2024). Learning from the ground up: lessons from civil society engagement in addressing the human rights implications of cybercrime legislation. *Journal*

of Cyber Policy, *9*(2), 131–148. https://doi.org/10.1080/23738871.2023.2240331

Bardhan, R., & Singh, A. (2023). Closing Legal disparities: The contribution of international bodies in unifying cyber legislation for enhanced cybersecurity. *Educational Administration: Theory and Practice*, 965–972. https://doi.org/10.53555/kuey.v29i3.7576

Bendiek, A., & Maat, E. P. (2019). The EU's regulatory approach to cybersecurity. German Institute for International and Security Affairs, Research Division EU Working Paper. https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pande

Big Brother Watch and Others v. United Kingdom, Applications Nos. 58170/13, 62322/14 and 24969/15, European Court of Human Rights (Grand Chamber, May 25, 2021).

Billow, J. (2023). No country is an island: Embracing international law enforcement cooperation to reduce the impact of cybercrime. Journal of Cyber Policy, 9(2), 149–158. https://doi.org/10.1080/23738871.2023.2245417

Blind, K., Niebel, C., & Rammer, C. (2023). The impact of the EU General Data Protection Regulation on product innovation. *Industry and Innovation*, *31*(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858

Brenner, S. W., & Koops, B. J. (2004). Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, Vol. 4, No. 1. Available at SSRN: https://ssrn.com/abstract=786507

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), 408–433. https://doi.org/10.1108/13639510610684674

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55–119.

Calcara, G. (2020). Balancing international police cooperation: INTERPOL and the undesirable trade-off between rights of individuals and global security. *Liverpool Law Review*,

42(2), 111–142. https://doi.org/10.1007/s10991-020-09266-9

Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. Monash University Law Review, 40(3), 698–736.

Council of Europe. (1949). Statute of the Council of Europe (ETS No. 1). London, 5 May 1949.

Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Daskal, J. (2015). The un-territoriality of data. Yale Law Journal, 125(2), 326–398.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. Telecommunications Policy, 39(9), 761–770.

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238 (Court of Justice of the European Union, April 8, 2014).

Doyle, S. (2022). *Why global harmonisation of cybersecurity would be music to everyone's ears*. World Economic Forum. Retrieved from https://www.weforum.org/stories/2022/03/why-global-harmonisation-of-cybersecurity-regulations-would-be-like-music-to-our-ears

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice. American Journal of International Law, 112(4), 583–657. https://doi.org/10.1017/ajil.2018.86

European Union Agency for Cybersecurity (ENISA). (n.d.). Who we are. https://www.enisa.europa.eu/about-enisa/who-we-are

Gastorn, K. (2017). Relevance of International Law In Combating Cybercrimes: Current Issues and Aalco's Approach. In *Presentation at the 4th World Internet Conference*,

Wuzhen Summit, on the Session on "International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes", 4th December. https://www.aalco.int/WIC%20-%20%20Cybercrimes%20-%2027.12.17.pdf

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Granger, M.-P., & Irion, K. (2014). The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU legislator and teaching a lesson in privacy and data protection. European Law Review, 39(6), 835–850.

Greenleaf, G. (2009). Five years of the APEC Privacy Framework: Failure or promise? Computer Law & Security Review, 25(1), 28–43.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India, August 24, 2017).

Klonick, K. (2018). The new governors: The people, rules, and processes governing online speech. Harvard Law Review, 131(6), 1598–1670.

Koskenniemi, M., & Leino, P. (2002). Fragmentation of international law? Postmodern anxieties. Leiden Journal of International Law, 15(3), 553–579.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, Article 102248.

Lessig, L. (2006). Code: Version 2.0. Basic Books. https://ia601903.us.archive.org/33/items/Code2.0/Code.pdf

Li, X. (2007, September 26). *International Actions Against Cybercrime: Networking Legal systems in the Networked Crime scene*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2281502

Masters, R. (2022). A comparison between the ACHPR Declaration of Principles on Freedom of Expression in Africa (2002) and

the Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019). Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/bueros/africa-media/20223.pdf

Mavenjina, M. (2018). African Union: A guide for human rights defenders. Kenya ICT Action Network. From https://www.kictanet.or.ke/african-union-a-guide-for-human-rights-defenders/

Milik, P. (2019). International legal regulations in the area of cybersecurity. *Cybersecurity and Law*, *1*(1), 115–141. https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-issn-2658-1493-year-2019-volume-1-issue-1-article-oai_editorialsystem_com_article-133774/c/articles-1991280.pdf.pdf

Mitrany, D. (1948). The functional approach to world organization. International Affairs, 24(3), 350–363. https://doi.org/10.2307/3018652

Neethu, N. (2020). Role of international organisations in prevention of cyber-crimes: An analysis. ResearchGate. https://www.researchgate.net/publication/350525198

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action.' *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Novas-Pena, A. N. (2024). Lack of international cyberspace regulation threatens human rights and international security. *HRRC*. https://www.humanrightsresearch.org/post/lack-of-international-cyberspace-regulation-threatens-human-rights-and-international-security

OECD. (1960). Convention on the Organisation for Economic Co-operation and Development. Paris, 14 December 1960 (in force 30 September 1961).

OECD. (2002). Recommendation of the Council concerning guidelines for the security of information systems and networks: Towards a culture of security

(OECD/LEGAL/0312). https://legalinstruments.oecd.org/public/doc/116/116.en.pdf

OECD. (n.d.). Members and partners. https://www.oecd.org/en/about/members-partners.html

Organisation for Economic Co-operation and Development. (1980). Guidelines governing the protection of privacy and transborder flows of personal data. OECD. https://doi.org/10.1787/9789264055375-en

Orji, U. J. (2018). *The African Union Convention on Cybersecurity: A regional response towards cyber stability?* Questa Soft. https://www.ceeol.com/search/article-detail?id=888733

Peters, A., & Jordan, A. (2019). *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*. Third Way. http://www.jstor.org/stable/resrep20150

Raul, A. C. (Ed.). (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited. https://datamatters.sidley.com/wp-content/uploads/sites/2/2019/11/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6.pdf

Rossini, C., & Green, N. (2015). Cybersecurity and human rights. *Global Partners Digital*. https://www.gp-digital.org/wp content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, 29(2), 353–400.

Singh, D. (2023). Cybersecurity and human rights: a complex interplay. *International Journal of Science and Research (IJSR)*, *12*(6), 1110–1112. https://doi.org/10.21275/sr23608234858

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum, 23(1), 101–108.

Tele2 Sverige AB v. Post- och telestyrelsen, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970 (Court of Justice of the European Union, December 21, 2016).

Tropina, T. (2024). 'This is not a human rights convention!': The perils of overlooking human rights in the UN cybercrime treaty. Journal of Cyber Policy, 9(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517

United Nations General Assembly. (2024). United Nations Convention against Cybercrime (Resolution 79/243). https://digitallibrary.un.org/record/4070329

UNODC. (n.d.-a). Cybercrime. https://unodc.org/unodc/en/cybercrime/index_new.html

UNODC. (n.d.-b). Cybercrime repository. https://unodc.org/unodc/en/cybercrime/cybercrime-repository.html

Ünver, H. A., & Kim, G. (2022). *Data privacy and surveillance in Turkey: an assessment of the draft law on the protection of personal data*. Centre for Economics and Foreign Policy Studies. Retrieved from https://www.jstor.org/stable/resrep14052

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Waters, N. (2009). The APEC Asia-Pacific Privacy Initiative: A new route to effective data protection or a Trojan horse for self-regulation? SCRIP Ted, 6(1). https://doi.org/10.2966/scrip.060109.75

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*(1–2), 63–72. https://doi.org/10.1365/s43439-020-00012-5