**Cybersecurity Policies Without Borders**

Jomael Ortiz Perez

Columbia Southern University

Table of Contents

[Introduction 3](#_Toc154597960)

[Who can make the laws applicable to cyberspace and cybersecurity? 5](#_Toc154597961)

[What laws apply once cybercrime crosses national and international boundaries? Why are they important? 9](#_Toc154597962)

[Who creates policy and enforces these laws? 11](#_Toc154597963)

[Conclusion 13](#_Toc154597964)

[References 16](#_Toc154597965)

# Introduction

In the digital age, cyberspace transcends traditional national boundaries, creating a complex and ever-evolving landscape that challenges conventional notions of governance, law enforcement, and international cooperation. Unlike the physical world, where geographical borders define jurisdictions, the virtual environment of the Internet presents a unique paradigm where activities, interactions, and crimes can originate and impact globally, irrespective of physical locations.

The need for a robust and cohesive framework to govern this space becomes paramount as the Internet becomes increasingly integral to global commerce, communication, and entertainment. This necessity is further accentuated by the rising incidence of cybercrime, which poses significant threats to individual privacy and security, national security, and the global economy.

The governance of cyberspace and cybersecurity thus demands an intricate balance of national interests, international cooperation, and adherence to universal principles of justice and fairness. Laws and regulations must evolve continuously to keep pace with the rapid advancement of technology and the innovative tactics employed by cybercriminals.

This paper delves into the multifaceted aspects of cyberspace governance, starting with examining the entities responsible for creating laws and regulations in this domain. It explores the roles and responsibilities of national governments, international organizations, and industry groups in shaping the legal landscape of cyberspace. The focus then shifts to the challenges and mechanisms of addressing cybercrime that crosses national and international boundaries, highlighting the significance of international treaties, conventions, and mutual legal assistance in fostering cross-border legal cooperation and law enforcement.

Moreover, the paper scrutinizes the entities that create policies and enforce laws in cyberspace, encompassing the efforts of national agencies, international bodies, law enforcement agencies, and the private sector. This comprehensive analysis aims to provide insights into the complexities of cyberspace governance and underline the importance of collaborative efforts in securing the digital world.

In this context, the paper also presents detailed case studies, including the Sony Pictures hack of 2014 and the WannaCry ransomware attack of 2017, to exemplify the real-world implications of cyber threats and the responses they necessitate. These case studies illustrate the practical challenges and successes in implementing cybersecurity measures and international cooperation.

This paper offers an in-depth understanding of the current state of cyberspace governance, the evolving nature of cyber threats, and the collaborative efforts required to create a secure and resilient digital future.

# **Who can make the laws applicable to cyberspace and cybersecurity?**

National governments play a crucial role in formulating and implementing laws and regulations that govern cyberspace and cybersecurity within their jurisdictions. This role is multifaceted and involves balancing the protection of citizens, infrastructure, and national interests with promoting innovation, privacy, and freedom of expression. For example, in the United States, the Computer Fraud and Abuse Act (CFAA) was enacted in 1986 as one of the earliest laws to address computer crime. Originally intended to protect government computers and financial institutions, it has since been amended to cover a broader range of computer-related offenses. The key provisions of the CFAA include prohibiting unauthorized computer access, which encompasses exceeding authorized access. The Act extends its protection beyond government and financial institutions to any computer used in or affecting interstate or foreign commerce or communication. Offenses under the CFAA range from computer trespassing and theft of information to damaging computers through the introduction of malware and denial of service attacks. Penalties vary based on the nature and severity of the offense and can include fines, imprisonment, or both. In cases of damage or theft, the penalties can be substantial.

However, the CFAA has faced criticism for its broad and vague terms, such as "unauthorized access," leading to debates over what constitutes a violation. There is an ongoing discussion about reforming the Act to balance better the need for security with protecting civil liberties.

The European Union's General Data Protection Regulation (GDPR), implemented in May 2018, represents one of the most significant global overhauls of data protection laws. The GDPR applies to all companies processing and holding subjects' data in the European Union, regardless of the company's location. Its fundamental principles include explicit and affirmative consent for processing personal data, the right of individuals to access their data and information about how it is processed, data portability, allowing individuals to obtain and reuse their data across different services, and the right to be forgotten, whereby data subjects can have the data controller erase their data. Data Protection Officers (DPOs) are required in specific organizations to oversee GDPR compliance. Non-compliance with GDPR can lead to heavy fines, up to 4% of annual global turnover or €20 million, whichever is greater. Other nations, such as China, with its Cybersecurity Law of 2017, focus on protecting personal information and individual privacy, mandating cybersecurity practices for network operators. Australia's Cybercrime Act 2001, amended in 2012, criminalizes unauthorized access, modification, or impairment of data and computer systems, with provisions for extraterritorial jurisdiction.

Challenges and considerations in this area include balancing security and privacy, the rapid pace of technological evolution often outstripping legislative processes, and the international implications of laws due to the global nature of the Internet, which necessitate international coordination and cooperation.

International organizations also play a pivotal role in shaping global policies and standards for cyberspace and cybersecurity. Their influence extends through setting norms, facilitating cooperation, and providing platforms for dialogue among nations. The Council of Europe's Budapest Convention, adopted in 2001, is the first international treaty to address Internet and computer crime by harmonizing national laws, improving legal authorities for investigative techniques, and increasing cooperation among nations. Its key provisions include criminalizing offenses against computer data and systems' confidentiality, integrity, and availability, offering guidelines for collecting electronic evidence and preserving data, and facilitating extradition and mutual legal assistance among signatory countries. However, not all countries have signed the Convention, partly due to concerns over sovereignty and privacy. The United Nations (UN), through initiatives like the Global Cybersecurity Agenda (GCA) launched by the International Telecommunication Union (ITU), provides a comprehensive framework for international cooperation to enhance confidence and security in the information society. The Internet Governance Forum (IGF) offers a platform for multi-stakeholder dialogue on public policy issues related to critical elements of Internet governance.

The World Trade Organization (WTO) plays a role in digital trade, addressing e-commerce and digital trade issues that indirectly affect cyberspace governance. Its Information Technology Agreement (ITA) is an agreement to eliminate tariffs on certain IT products, impacting the global digital economy.

Industry groups and coalitions are increasingly significant in shaping cyberspace, often driving innovation and standards that influence global cybersecurity practices. The Payment Card Industry Security Standards Council (PCI SSC) enforces the PCI Data Security Standard (PCI DSS), a set of security standards ensuring that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Compliance is mandatory for all entities handling credit card transactions. The standard significantly impacts how businesses globally handle payment security, though it is not a governmental regulation. The Internet Engineering Task Force (IETF) develops and promotes voluntary Internet standards, particularly in Internet protocol (IP), playing a crucial role in the operational management of the Internet. Its notable contributions include the standards for TCP/IP, forming the foundation of Internet communications. The International Organization for Standardization (ISO), with its ISO/IEC 27000 series, widely recognized and adopted by organizations worldwide, helps secure information assets, influencing cybersecurity practices beyond national boundaries. The Global Cyber Alliance (GCA) is an international, cross-sector effort to reduce cyber risk and improve our connected world, focusing on mitigating systemic cybersecurity risks and providing practical, measurable solutions.

The challenges of standardization versus flexibility, public-private partnerships, and keeping pace with innovation are central to the broader implications of this field. Balancing the need for standardized global protocols with the diverse requirements and conditions of different regions and industries is essential. Encouraging collaboration between the private sector and government agencies is crucial for more effective cybersecurity measures. As industry standards and practices must evolve with rapidly advancing technologies, the entire sphere of cyber governance remains dynamic and ever-changing.

# **What laws apply once cybercrime crosses national and international boundaries? Why are they important?**

Transnational cybercrime presents significant challenges due to its cross-border nature, demanding coordinated international efforts for effective management and resolution. The sophistication of cybercriminals and the global nature of the Internet require robust mechanisms for international legal cooperation and harmonization. The Budapest Convention plays a crucial role in this arena, facilitating extradition between member states for cybercrimes and providing a framework for mutual legal assistance, which is essential in investigations and prosecutions involving multiple jurisdictions. It also emphasizes capacity building to enhance member states' abilities to combat cybercrime through training and resource sharing.

Additionally, international agreements like the United Nations Convention Against Transnational Organized Crime, while not explicitly focused on cybercrime, offer essential frameworks for cooperation against organized crime, which increasingly involves cyber elements. Regional agreements, such as the African Union Convention on Cyber Security and Personal Data Protection, address specific regional challenges in cybercrime.

Mutual Legal Assistance Treaties (MLATs) are critical in cybercrime investigations as they involve agreements between countries to gather and exchange information for enforcing laws. However, the process can be time-consuming due to the fast-paced nature of digital evidence, highlighting the need for streamlined procedures. National laws with extraterritorial application also play a significant role. For instance, the U.S. Computer Fraud and Abuse Act (CFAA) applies to non-U.S. citizens if the cybercrime involves U.S. systems or significantly impacts U.S. interests. The EU's Directive on Attacks against Information Systems (2013) allows for jurisdiction over offenses committed against any EU member state or by its nationals.

The role of international law enforcement agencies is pivotal in addressing transnational cybercrime. Agencies like Interpol's Cyber Fusion Centre and Europol's European Cybercrime Centre (EC3) provide platforms for rapid information exchange and coordination among countries, enhancing the collective response to cyber threats. However, challenges such as jurisdictional complexities and differences in legal frameworks across countries can hinder cross-border investigations.

Additionally, the rapidly evolving nature of cyber threats necessitates constant adaptation of legal and operational strategies.

Emerging trends in this domain include increased international cooperation and information sharing, with more countries participating in global agreements. Cyber diplomacy is also gaining recognition as a critical aspect of addressing cybersecurity issues, creating specialized diplomatic positions and departments focused on cyber affairs.

# **Who creates policy and enforces these laws?**

Creating and enforcing cyberspace and cybersecurity policies is a complex task that involves the intricate interplay between national governments, international bodies, law enforcement agencies, and the private sector. This multifaceted process is essential for ensuring a secure and resilient digital world. National governments are pivotal in this endeavor, primarily responsible for developing and implementing cybersecurity and data protection policies within their jurisdictions. They are crucial in legislating, regulating, and enforcing digital activities and cybersecurity laws. For instance, in the United States, comprehensive cybersecurity policies have been established through legislation, executive orders, and national strategies, with the National Cyber Strategy providing a clear roadmap for protecting American networks and enhancing national cybersecurity. Key enforcement agencies in the U.S. include the FBI's Cyber Division, which counters cybercrime and protects against cyber-based terrorism and espionage, and the Cybersecurity and Infrastructure Security Agency (CISA), which focuses on protecting the nation's critical infrastructure.

The European Union also demonstrates a solid commitment to cybersecurity, with its Cybersecurity Strategy encompassing directives like the NIS Directive, which sets network and information security requirements across member states. The EU Agency for Cybersecurity (ENISA) is instrumental in implementing the EU's cybersecurity strategy alongside national cybersecurity authorities.

International bodies contribute significantly to policy creation by setting standards, facilitating dialogues, and providing platforms for international cooperation. The United Nations, for example, through various agencies and forums, works on setting global norms and standards for cybersecurity and internet governance. One such initiative is the Group of Governmental Experts (GGE) on Advancing Responsible State Behavior in Cyberspace in the Context of International Security. These organizations provide technical assistance and capacity-building resources, particularly to developing countries.

Law enforcement agencies require cross-border cooperation and coordination to enforce cyber policies effectively. Interpol's Global Cybercrime Program combats cybercrime through a global network, offering tools, training, and support in cybercrime investigations. Similarly, Europol's European Cybercrime Centre (EC3) is a central hub in the EU's fight against cybercrime, supporting member states in their investigations and developing prevention and awareness campaigns.

Given its expertise and resources, the private sector's involvement in policy creation and enforcement is increasingly recognized as critical. Businesses often use information-sharing initiatives like Information Sharing and Analysis Centers (ISACs) to exchange threat intelligence and collaborate with governments to develop effective cybersecurity strategies.

However, significant hurdles include harmonizing international cybersecurity and data protection laws, keeping pace with rapid technological changes, and balancing security with privacy. Emerging trends in cybersecurity policy focus on increasing cyber resilience, preparing for, responding to, and recovering from cyber-attacks, and recognizing cybersecurity as a crucial component of national security, economic stability, and public safety.

# Conclusion

This paper's exploration of cyberspace governance, laws, and enforcement underscores the intricate and evolving nature of managing digital spaces and combating cyber threats. As we have delved into the multifaceted roles of national governments, international organizations, and industry groups, it becomes evident that governing cyberspace is not confined to a single entity but is a collective responsibility shared across various sectors and borders.

The dynamic interplay of national laws, such as the United States' CFAA and the European Union's GDPR, with international conventions like the Budapest Convention, illustrates the complexity of legal frameworks required to address the transnational nature of cyber activities. These laws and agreements form the backbone of our defense against cybercrime, providing mechanisms for cooperation and legal recourse in a domain where perpetrators often operate beyond the reach of traditional law enforcement.

The case studies of the Sony Pictures hack and the WannaCry ransomware attack highlight the global impact of cyber threats and the critical need for coordinated international response and public-private partnerships. These incidents demonstrate that cybersecurity is a national concern and a global imperative, necessitating a unified approach to safeguarding our interconnected digital world.

In reflecting upon the roles of various agencies and organizations in enforcing cyber laws, from the FBI and DHS in the United States to Interpol and Europol on the international stage, the significance of collaborative efforts in intelligence sharing, investigation, and response to cyber incidents is abundantly clear. The private sector, too, plays a pivotal role, not just in compliance with laws and regulations but also in proactive threat detection and sharing of critical cybersecurity intelligence.

Moving forward, it is paramount that legal frameworks continue to adapt to the ever-changing landscape of technology and cyber threats. The legal, ethical, and logistical challenges posed by emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) will require innovative and forward-thinking approaches to regulation and enforcement.

Moreover, fostering a cybersecurity awareness and education culture is crucial in building a resilient digital ecosystem. Individuals, organizations, and governments must all play their part in enhancing cyber hygiene and awareness to mitigate the risk of cyber attacks.

In conclusion, cyberspace governance is a complex, multifaceted endeavor that demands ongoing adaptation, international cooperation, and a commitment to innovation and education. As we navigate the challenges and opportunities the digital age presents, the collective effort and collaboration across nations, industries, and communities will pave the way for a secure, stable, and prosperous digital future.

# References

(2019). United States : Guidewire Achieves Payment Card Industry Data Security Standard (PCI-DSS) Compliance and is Named a Visa Third-Party Agent. MENA Report, (),.

(2021). Korea Republic of: Ministry of Foreign Affairs Holds 3rd Inter-Regional Conference on Cyber/ICT Security Together with OSCE. MENA Report, (),.

Bhola, P., Bhola, P., Kotsampopoulos, P., Kotsampopoulos, P., & Hatziargyriou, N. (2023). Business Model Selection for Community Energy Storage: A Multi Criteria Decision Making Approach. Energies, 16(18), 6753.

Danay Tinawin, R. (2022). The development of a sustainable framework for an industry driven career-focused ICT curriculum in producing sought after ICT graduates. https://core.ac.uk/download/576566740.pdf

Flores‐Toro, J., Go, K. L., Leeuwenburgh, C., & Kim, J. S. (2016). Autophagy in the liver: Cell's cannibalism and beyond. Archives of Pharmacal Research. https://doi.org/10.1007/s12272-016-0807-8.

Lewis, T. G. (2019). Critical Infrastructure Protection in Homeland Security (3rd ed.). Wiley Global Research (STMS). https://online.vitalsource.com/books/9781119614562