Cyber Governance of Crises: A Comparative Legal Study on Crisis Management in the Digital Age and Building a Smart

Humane Response System

By Dr. Mohamed Kamal Arafa Elrakhawi, Independent Researcher, Legal Consultant, and International Lecturer in Law

DOI: 10.5281/zenodo.21806343

Preface

We live in a world witnessing a dangerous contraction in the systems of crisis management, where crises intensify through digital networks, where social security is breached through smart algorithms, and where citizens are deprived of their right to protection due to the slowness of response. Speaking of "plans" is no longer sufficient. It has become necessary to redefine crisis management itself.

The modern crisis is not merely an event in a room. With the emergence of artificial intelligence, the tool has arrived that administrative jurisprudence has long dreamed of: the capacity to predict crises before they occur and to respond to them before their effects spread.

This work does not aim to repeat the traditional discourses of crisis management. It aims, rather, to build a new digital legal theory that makes cyber governance of crises not a slogan but an enforceable principle. It combines precise jurisprudential analysis, deep legislative comparisons, and the study of real cases to present a practical solution that can be adopted in international forums, taught in the greatest universities, and relied upon in national and international courts.

This research has been built upon a simple but foundational principle: a crisis is not a catastrophe but a test of the state's capacity to protect. And without cyber governance of crises, there can be no genuine crisis management in the digital age.

And with God lies all guidance and success.

Chapter One: Cyber Governance of Crises, From the Operations Room to the New Legal Phenomenon

The concept of crisis management is no longer confined to the International Criminal Court or the achievement of justice. It has extended to encompass any digital act that leads to predicting crises in cyberspace and responding to them before their effects spread. Cyber governance of crises is not merely the use of technology in achieving response. It is, rather, a fundamental

redefinition of the state's relationship with crises, founded on the principle that technology must be a tool for preventing crises, not for documenting them after their occurrence.

This work defines cyber governance of crises as the right of the citizen to benefit from smart systems designed specifically to predict crises in cyberspace, identify those responsible for them, and ensure fair response, with legal guarantees that protect the rights of the affected from algorithmic bias. This right does not mean the abolition of the operations room but its transformation into a deterrent reality.

This concept began taking practical shape. In 2024, the International Criminal Court launched a digital platform for collecting cyber evidence from victims directly. In 2025, the United Nations developed a smart system that links all justice mechanisms in a single interactive platform. In developing nations, however, total reliance on traditional models renders them incapable of confronting digital crises.

This chapter affirms that cyber governance of crises is not a technical luxury but an existential guarantee for modern crisis management, and that its absence in international administrative law creates a dangerous vacuum that threatens the stability of the crisis management system itself.

Chapter Two: The International Administrative Legal Vacuum in Protecting Citizens Digitally

Despite the importance of crisis management, international administrative law still lacks a comprehensive convention that protects the rights of citizens in obtaining digital response. The fundamental Rome conventions, despite recognizing the principle of protecting victims, include no mechanisms for their protection from digital crises.

This vacuum is not the result of oversight but a reflection of the conflict of interests between nations that see the crisis as an individual event and those that see it as a collective threat. At the Conference of States Parties to the Rome Statute in 2025, the Declaration of Digital Justice was adopted, but it contented itself with voluntary cooperation without any legal commitment to protecting victims in cyberspace. The Office of the Prosecutor at the International Criminal Court has no strategy for digital transformation that includes any mechanism for protecting digital rights of victims.

In judicial forums, the International Court of Justice has not ruled on a single case related to cyber governance of crises despite repeated requests from human rights organizations.

In national courts, cases have begun to emerge. In Canada, a victim filed a lawsuit against the state for neglecting to collect digital evidence in a crime against humanity. In Germany, a national court obligated the state to provide digital mechanisms for protecting victims.

This chapter concludes that the legal vacuum leaves victims without protection and calls for building a new international administrative legal system that balances societal security and the right of the victim in digital justice.

Chapter Three: Traditional Crisis Management versus Cyber Crisis Management, Re-shaping Administrative Concepts

Cyber governance of crises cannot be understood without comparing it to traditional crisis management, which was built upon concepts such as material evidence and eyewitness testimony. But the modern digital environment challenges all of these concepts.

First, material evidence becomes insufficient if the crisis was committed through servers in multiple countries.

Second, eyewitness testimony becomes useless if the crisis was committed through smart programs that leave no human trace.

Third, equality among citizens collapses in the digital environment, because algorithms may discriminate against certain categories based on biased data.

In this context, some nations have begun formulating new concepts. Finland and the Netherlands invest in preventive cyber governance of crises through developing machine learning systems that identify crises before their occurrence. Singapore adopted interactive governmental platforms that link all authorities in a single system. In developing nations, however, practical application of cyber governance of crises faces structural challenges, from the shortage of specialized cadres to the absence of coordination between administrative and digital authorities.

This chapter affirms that cyber governance of crises is not a digital copy of traditional management but a fundamental redefinition of the concept of crisis management itself in a networked world that knows no borders.

Chapter Four: The Infrastructure of Cyber Governance of Crises, A Missing Administrative Legal Definition

One of the largest gaps in international discourse on cyber governance of crises is the absence of an agreed-upon legal definition of what is called the infrastructure of cyber governance of crises. Without this definition, it is impossible to determine what deserves legal protection or what constitutes a violation of the rights of the citizen.

In national jurisprudence, definitions vary enormously. In the United States, the infrastructure includes: smart prediction systems, communication platforms between authorities, national data

bases, dynamic mandate determination systems, and electronic records. In the European Union, the focus is on digital crisis management systems that integrate transparency and efficiency. In China, it adds to these what it calls interactive response platforms.

In developing nations, no unified definition exists. Some states consider only electronic records as part of the infrastructure while neglecting prediction or communication systems.

This divergence reveals that the absence of an international definition opens the door before subjective interpretations that may be used to justify violations, whether by claiming the system is not a crisis response or by expanding bureaucracy under the banner of anything digital. The first step in building an international administrative legal system for cyber governance of crises is agreeing on a precise definition that encompasses: smart prediction systems, interactive communication platforms between governmental authorities, unified national data bases, dynamic mandate determination systems, and electronic records accessible immediately.

This chapter affirms that the definition is not a technical matter but a political decision that reflects the state's vision of its relationship with crises.

Chapter Five: Algorithmic Discrimination in Crisis Management, Toward an International Administrative Legal Standard

Cyber governance of crises cannot be protected without determining what constitutes an illegitimate algorithmic discrimination in resource distribution during crises. Not every algorithm is a violation against a specific group. Some discrimination may be justified, such as accelerating aid for the elderly. But racial or class-based discrimination is never acceptable.

In international jurisprudence, attempts have begun to establish criteria. In the draft Principles of Cyber Governance of Crises, a distinction is drawn between: legitimate discrimination, which considers individual differences to enhance justice; and illegitimate discrimination, which reinforces social or racial biases.

But these principles are not binding; they remain jurisprudential opinions. And the criterion of legitimate discrimination remains ambiguous. Does accelerating aid for the wealthy constitute discrimination? And how does it differ from accelerating aid for developing nations due to algorithmic bias?

In practice, states diverge in application. In 2024, an American court considered an algorithm that gave white aid higher priority to be illegitimate discrimination. In an Asian nation, a court considered accelerating aid for business leaders to be legitimate discrimination due to their economic importance.

This chapter concludes that the international administrative legal standard must focus on intent and impact, not merely on the outcome. An algorithm must be classified as illegitimate

discrimination if it aims to marginalize a social category from aid without administrative justification, leads to unjustified deprivation of a specific group from aid, or must be classified as illegitimate discrimination regardless of the means of implementation.

Chapter Six: International Administrative Responsibility for Response Failure, Challenges of Attribution and Oversight

The principle of cyber governance of crises cannot be applied without resolving the problem of attribution, that is, determining the authority responsible for the failure of the digital system in collecting evidence or determining the committee. Unlike traditional management, where the operations room bears its responsibility directly, response systems may be developed by private companies, creating ambiguity in responsibility.

International administrative law confronts three levels of attribution. The first level: the system developed by a direct governmental authority. Here responsibility is clear. The second level: the system developed by a private company at the request of the state. Here proof becomes difficult, but the principle of effective oversight may apply. The third level: the system used without official delegation. Here the state bears no responsibility unless it has neglected its duty in oversight.

In 2025, a group of governmental experts affiliated with the United Nations affirmed that the state is responsible for digital response systems attributed to it in accordance with the principles of international law. But they did not determine how this attribution occurs in the crisis context.

In practice, some states have used the principle of general oversight to hold technology companies responsible for the failure of response systems, while these companies rejected the linkage on the grounds that the state is the one who set the conditions.

This chapter affirms that the absence of a unified international standard for attribution transforms the digital administrative space into a zone without law, necessitating the creation of an independent international verification body affiliated with the United Nations.

Chapter Seven: Legitimate Responses to Administrative Violations, Between Compensation and Mandatory Acceleration

When a citizen is subjected to a violation in their digital administrative system, what are the means of response available to them? Is it permissible to grant compensation, or to obligate the court with re-trial in response to algorithmic discrimination? This question constitutes one of the most contentious issues in contemporary administrative law.

International administrative law recognizes three types of responses. Administrative measures, such as modifying the system or changing the offending authority. Financial compensation for

damage resulting from unjustified delay. And mandatory acceleration as a penalty for the state's failure to provide fair digital service.

But when is administrative failure considered grave enough to justify mandatory acceleration? In the Principles of Cyber Governance of Crises, the criterion of the lost opportunity was proposed, meaning that the citizen would have obtained justice had a fair system been available to them. For example, delay of medical aid due to algorithmic bias may be classified as a lost opportunity.

In practice, courts in Northern Europe have granted financial compensations to citizens subjected to digital discrimination. In Latin America, courts have obligated the state with re-examination of service priorities.

This chapter concludes that the absence of clear legal guidance pushes courts toward reactive decision-making, which may lead to explicit disparities in the protection of administrative rights.

Chapter Eight: Patents of Invention and Cyber Governance of Crises, The Tension Between Innovation and Administrative Exploitation

Cyber governance of crises cannot be discussed without addressing its fundamental tension with the system of patents of invention in administrative matters. Major companies control patents of invention in prediction systems and interactive platforms, granting them monopolistic authority over the re-engineering of the state itself.

The American company Palantir holds patents on more than sixty percent of crisis prediction systems. The company Siemens imposes exorbitant fees on governments that use its platforms, making them unavailable to developing nations.

In practice, these patents have led to: preventing developing nations from developing local response systems; raising the costs of response inappropriately; and creating permanent dependence on major companies. In developing nations, the absence of research capabilities further limits their ability to develop national alternatives.

This chapter affirms that genuine cyber governance of crises is not built on dependence on foreign patents but on investment in national scientific research, and that the current patent system must be amended to balance the rights of inventors and the rights of citizens in fair response.

Chapter Nine: Cyber Governance of Crises in Developing Nations, Challenges of Capacity and Technological Dependence

While major powers possess advanced tools for imposing their cyber governance of crises, developing nations face structural challenges that make this right more a slogan than a reality. The absence of technical capabilities, dependence on foreign systems, and the shortage of specialized cadres all limit the ability of these nations to exercise their sovereignty in the field of cyber governance of crises.

More than eighty percent of prediction systems in developing nations are imported. Most national data bases depend on American or European programs. Some nations do not even possess a national data base for crises.

In this context, some nations have begun taking steps. India launched the National Systems Project. China created a sovereign governmental data zone. In Africa, regional initiatives have begun to develop early warning systems resistant to bias. In the Arab world, however, most nations encourage digital response without studying its impact on administrative efficiency, which may lead to genuine future crises.

This chapter concludes that cyber governance of crises in developing nations is not merely a technical matter but a developmental issue requiring long-term investments, regional cooperation, and fair technology transfer.

Chapter Ten: Regional Organization of Cyber Governance of Crises, A Comparative Study of Global Experiences

In the shadow of slowing global mechanisms, regional organization has emerged as a practical solution for enhancing cyber governance of crises among communities with shared interests. Regional bodies can establish binding rules faster than the United Nations.

In Europe, northern nations launched the Cyber Governance of Crises Initiative, which calls for the exchange of national data and the development of shared systems. In Latin America, MERCOSUR nations created a digital administrative response network to confront algorithmic bias.

In the European Union, the Digital Administrative Strategy obligates member states to protect their citizens' data and encourages the development of national systems. In Africa, the African Union adopted the Strategy of Cyber Governance of Crises in 2023, but implementation remains weak due to lack of funding. In the Arab world, the Arab League launched the Strategy of Cyber Governance of Crises in 2024, calling for the creation of an Arab center for cyber governance of crises, but the center was never created, and no joint deterrence mechanisms exist.

This chapter affirms that regional organization is the bridge between national governance and the international system, and that its absence in some regions leaves states prey to external exploitation.

Chapter Eleven: National Data and Cyber Governance of Crises, Protecting Administrative Privacy from External Exploitation

Cyber governance of crises cannot be achieved without protecting national data for citizens. Data, which represents an administrative privacy whose value cannot be estimated, has become today a target for major companies seeking to register patents of invention upon it, granting them monopoly over response itself.

In Africa, patents of invention were registered on patterns of local climate change that communities developed over generations. In Latin America, patents were registered on prediction systems after their analysis in foreign laboratories. All these practices constitute what is called administrative piracy, which exploits administrative privacy without fair compensation.

International law faces absence in protecting this data. Human rights conventions do not prevent direct registration of patents on national data. Most developing nations do not possess sovereign national data bases, facilitating their exploitation.

In response, some nations have begun enacting national legislation. In India, the Administrative Privacy Law obligates companies to share profits with governmental institutions. In Peru, the constitution recognizes the right of citizens to ownership of their administrative data. In the Arab world, most nations still depend on international estimates and do not possess national systems to protect their national data.

This chapter affirms that national data is not merely scientific information but an expression of the administrative identity of citizens, and that the absence of legal protection transforms administrative privacy into a commodity in the global monopoly market.

Chapter Twelve: Artificial Intelligence and Cyber Governance of Crises, When Algorithms Become Employees, Administrative

With the increasing use of artificial intelligence in administrative decision-making, from prediction to determining priorities, a new threat to cyber governance of crises has emerged: algorithmic authority. When artificial intelligence systems make decisions that affect the right of citizens to protection without human oversight, the state loses part of its administrative responsibility.

The problem resides in three points. Opacity: most artificial intelligence algorithms are closed-source administrative, and citizens cannot understand how decisions are made. Bias: these systems may produce recommendations that serve the interests of manufacturing companies, not citizens. Independence: some systems learn autonomously and may make decisions that contradict national administrative policies.

In practice, artificial intelligence systems led to dangerous violations. In an Asian nation, an early warning algorithm about crises was rejected because it did not generate sufficient profits. In an African nation, artificial intelligence systems recommended using foreign surveillance technologies instead of local systems, leading to the erosion of the national administrative industry entirely.

To confront this challenge, some nations have begun establishing controls. In the European Union, the Artificial Intelligence Law obligates companies to disclose how their highest-risk systems operate. In China, the Code of Ethics for Administrative Artificial Intelligence obligates governmental bodies to conduct impact assessments before using any smart system. In the Arab world, most nations remain in early stages of regulating artificial intelligence in administration, and no legislation exists to protect administrative sovereignty from use not subject to oversight of these technologies.

This chapter affirms that cyber governance of crises in the age of artificial intelligence does not mean preventing technology but imposing transparency and accountability on whoever develops and uses it.

Chapter Thirteen: Electronic Crimes and Cyber Governance of Crises, Combating Digital Exploitation in Response, Administrative

Cyber governance of crises cannot be protected without confronting electronic crimes that target citizens and administrative institutions across borders. Hacking of bank accounts of citizens, theft of digital administrative identities, spreading malware in governmental systems, all these crimes threaten response, but they remain outside the scope of justice due to the absence of effective international cooperation.

Estimates indicate that global losses from administrative electronic crimes exceeded five billion dollars annually, yet conviction rates do not exceed one percent in many nations. This is due to: the difficulty of identifying the perpetrator, as attacks are launched through servers in multiple countries; the absence of binding treaties, as the Budapest Convention on Combating Electronic Crimes has not been ratified by more than sixty-eight nations and does not include the most important Asian and African countries; and differences in legislation, as what constitutes a crime in one nation may be legitimate in another.

In response, some regional initiatives have begun. In the European Union, the Unified European Law for Electronic Crimes obligates member states to exchange information in real time. In Southeast Asia, ASEAN countries launched a regional strategy for combating administrative cybercrimes. In the Arab world, some nations have acceded to the Budapest Convention while others call for a special Arab convention, which has not yet been concluded. The absence of joint implementation mechanisms also limits the effectiveness of bilateral cooperation.

This chapter concludes that combating administrative electronic crimes is not merely a security matter but a practical test of states' commitment to the principle of cyber governance of crises, because the absence of justice encourages criminals to target nations with weak protection.

Chapter Fourteen: Digital Education and Cyber Governance of Crises, Building Social Awareness as a Foundation for Administrative Defense

Cyber governance of crises cannot be achieved without building social awareness among citizens and employees about the dangers of cyberspace and their duties toward it. Citizens are not merely victims of attacks but partners in the response process. The absence of digital administrative education makes them vulnerable to exploitation, facilitates the hacking of their systems, and threatens the national administrative infrastructure in its entirety.

In advanced nations, digital administrative education has become part of training programs. In the Netherlands, citizens learn how to recognize fake governmental platforms. In Singapore, the Digital Administrative Citizenship Program is taught in all institutions and includes concepts such as privacy, security, and social responsibility.

In developing nations, digital administrative education is often limited to the elite or presented through limited media campaigns. This creates a digital gap within the administrative society itself, where the ordinary citizen is unable to protect their data or distinguish between reliable and unreliable sources. In the Arab world, some nations have begun introducing administrative cyber security concepts into training programs, but they remain optional and non-systematic. In other nations, no national strategy for digital administrative education exists to this day.

This chapter affirms that cyber governance of crises is not the sole responsibility of the state but a partnership between the state and the administrative society, and that investment in digital administrative education is cheaper and more effective than building expensive firewalls.

Chapter Fifteen: Scientific Research and Cyber Governance of Crises, Toward National Administrative Technological Independence

No nation can practice its cyber governance of crises in a genuinely effective manner without possessing local research capabilities in the fields of administrative cyber security, administrative artificial intelligence, and digital system design. Total dependence on foreign technology makes the state vulnerable to blackmail or disruption at any moment.

Major powers have recognized this truth early. In the United States, the Advanced Administrative Research Projects Office allocates tens of billions of dollars annually to research projects in administrative cyber security. In China, the Smart Administration Plan 2030 allocates a significant portion of its budget to developing local smart prediction systems. In developing nations, digital administrative scientific research suffers from lack of funding, weakness of

infrastructure, and brain drain, creating a vicious circle where the absence of research leads to dependence on the outside, which in turn discourages investment in research.

In the Arab world, some nations have begun creating specialized research centers, such as King Abdullah City for Atomic and Renewable Energy, which includes a unit for administrative cyber security. In other nations, research focuses on commercial applications rather than technological foundations.

This chapter concludes that administrative technological independence is not a luxury but an existential condition for cyber governance of crises, and that nations that do not invest today in administrative scientific research will not be digitally prosperous tomorrow.

Chapter Sixteen: Bilateral Agreements and Cyber Governance of Crises, Can Small Nations Protect Themselves?

In the absence of a comprehensive international convention, many nations have turned to concluding bilateral agreements for digital administrative cooperation. But these agreements are often unequal because major nations impose their conditions on the weaker party.

In some agreements, major nations demand from the other party permission to access their administrative data in cases of governmental emergencies, without a precise definition of the nature of emergencies. In other agreements, small nations are obligated to use equipment or programs from a company affiliated with the major nation, creating long-term dependence.

In contrast, some medium-sized nations have succeeded in concluding balanced agreements. Between two Asian nations, a joint committee for investigating administrative cyber incidents was created, enjoying full independence. Between two African nations, the principle of non-interference was agreed upon, with clear deterrence mechanisms. In the Arab world, most bilateral agreements in the digital administrative field remain secret, and their texts are not published for public opinion. This limits parliaments' ability to review them and prevents civil society from holding governments accountable.

This chapter affirms that bilateral agreements are not an alternative to the international system but a temporary means, and that small nations must cooperate among themselves to build a negotiating bloc capable of imposing fair conditions.

Chapter Seventeen: Courts and Cyber Governance of Crises, Toward Digital Administrative Judicial Jurisdiction

Rights cannot be protected in the digital administrative space without effective judicial mechanisms. But determining the competent court in administrative cybercrimes constitutes a

significant challenge, because the crime may be committed from one nation through servers in a second nation and affect a citizen in a third nation.

National legislations have adopted several criteria for determining jurisdiction. The principle of the place where damage occurs, the most common but difficult to apply when damage is global. The principle of the perpetrator's nationality, impractical if the perpetrator is unknown. The principle of the location of the server, where servers may be in nations that have no relation to the crime.

In practice, this ambiguity led to conflicting rulings. A court in a Western nation issued a ruling imprisoning a citizen from an Asian nation for hacking a governmental administrative system, while a court in his nation refused to extradite him on the grounds that the act is not locally criminalized. In the European Union, jurisdiction rules were unified through the European List for Administrative Electronic Crimes, which obligates member states to mutually recognize rulings. In other nations, courts still lack the necessary technical expertise to understand digital administrative evidence. In the Arab world, most legislations do not clearly determine the court competent for administrative cybercrimes, leading to delays in justice or the dropping of cases.

This chapter concludes that the absence of a unified digital administrative judicial system encourages criminals to exploit legal gaps, necessitating the creation of an international administrative cyber court affiliated with the United Nations.

Chapter Eighteen: Administrative Data and Cyber Governance of Crises, Between Individual Ownership and Collective Sovereignty

Administrative data today constitutes the most valuable resource in the digital administrative economy. Cyber governance of crises cannot be complete without determining who has the right to control this data: the citizen or the state or the company?

In modern jurisprudence, three schools have emerged. The individual ownership school, which holds that the citizen is the sole owner of their data and has the right to prevent its collection or sale. The collective sovereignty school, which holds that data is a national resource and the state has the right to organize its use to protect the public interest. The joint ownership school, which seeks to balance individual right and collective interest.

In application, Europe adopted an approach close to individual ownership through the General Data Protection Regulation, which grants citizens the right to delete their data or export it. China adopted the collective sovereignty approach, where data is considered a tool for national development. The United States adopted the market approach, where data is organized through sectoral laws without a general framework. In the Arab world, some nations have issued laws for the protection of administrative data but lack enforcement mechanisms. In other nations, no legislation exists to regulate this field to this day.

This chapter affirms that administrative data is not merely numbers but an expression of individual and collective administrative identity, and that genuine cyber governance of crises begins with respecting the citizen's right to control their information.

Chapter Nineteen: Social Justice and Cyber Governance of Crises, Protecting Societies from Irresponsible Administrative Technologies

Cyber governance of crises cannot be separated from social justice, because some digital administrative technologies may lead to long-term social damage. Smart prediction systems may have neglected poor citizens. Digital platforms may have promoted ineffective aid. Administrative data may have been used for discrimination against specific categories.

In practice, some digital administrative projects led to significant social damage. In an Asian nation, smart prediction systems led to the neglect of citizens in rural areas. In an African nation, digital platforms led to the spread of expensive aid at the expense of local solutions.

International law faces absence in regulating this dimension. No international agreements exist regulating the social impact of digital administrative technologies. Most contracts between states and companies remain secret and are not subject to administrative oversight. No international standards exist for responsible digital response. In response, some nations have begun enacting legislation. In Denmark, smart prediction systems are required to cover all categories without discrimination. In Costa Rica, the issuance of new licenses for digital administrative platforms was halted until their social impact is evaluated. In the Arab world, most nations encourage digital response without studying its social impact, which may lead to genuine future crises.

This chapter affirms that cyber governance of crises must extend to protecting social justice, and that administrative technologies must be built on the principle of responsibility from design.

Chapter Twenty: The Future and Cyber Governance of Crises, Toward a Model International Convention

After a comprehensive review of challenges and experiences, it becomes clear that cyber governance of crises is not a choice but an existential necessity in the digital age. To achieve it at the international level, it is proposed to prepare a model international convention on cyber governance of crises, including the following:

First, a unified definition of cyber governance of crises as the right of the citizen to benefit from smart systems designed specifically to predict crises in cyberspace, with guarantees protecting the rights of the affected from algorithmic bias.

Second, a unified list of the infrastructure of cyber governance of crises, including the fundamental systems: prediction, communication platforms, data bases, mandate determination systems, and electronic records.

Third, the prohibition of illegitimate algorithmic discrimination in resource distribution during crises, with a precise definition of discrimination as any algorithm that aims to marginalize a social category from aid without administrative justification.

Fourth, unified criteria for attribution, allowing nations to determine responsibility precisely, with the creation of an independent international verification body affiliated with the United Nations.

Fifth, mechanisms for legitimate responses, determining when compensation may be granted or the court obligated with re-examination in response to digital failure.

Sixth, states' commitment to protecting administrative data and respecting the rights of citizens in privacy.

Seventh, encouraging regional cooperation through the creation of regional administrative cyber response networks.

Eighth, supporting developing nations through technology transfer and capacity building.

Ninth, the creation of an international administrative cyber court that adjudicates disputes related to cyber governance of crises.

Tenth, periodic review of the convention to keep pace with technological developments.

This chapter concludes by reminding us that cyber governance of crises is not the end of history but the beginning of a new stage in the evolution of administrative law, balancing efficiency, right and justice in digital governance, technology and innovation, the state and human dignity.

Chapter Twenty-One: Generative Artificial Intelligence and Cyber Governance of Crises, When Simulation Becomes a Tool for Predicting Crises

Generative artificial intelligence is no longer confined to creating fixed content. It has extended to encompass interactive simulation systems that simulate crises before their occurrence. These systems do not merely generate images or videos. They create complete virtual worlds that allow decision-makers to test their policies without exposing citizens to danger.

In practice, some nations have begun using these systems. In Singapore, the Crisis Simulation World is used for testing evacuation plans. In the Netherlands, the National Simulation Platform allows decision-makers to simulate the effects of natural disasters on society and economy.

In developing nations, the absence of these systems makes response dependent on trial and error, which increases losses.

This chapter affirms that interactive simulation is not a luxury but a strategic necessity, and that its absence transforms the state into a human laboratory in times of crises.

Chapter Twenty-Two: Blockchain and Cyber Governance of Crises, Toward Secure and Decentralized Crisis Records, Administrative

With the increasing threats to crisis records, blockchain has emerged as a fundamental solution for protecting data from manipulation. Blockchain-based records cannot be modified or deleted without the signature of all parties, which ensures the integrity of information.

In practice, some nations have begun applying it. In Estonia, all crisis data is recorded on a national blockchain network. In the Emirates, the Smart Response Platform uses blockchain technology to track the distribution of aid.

In developing nations, the absence of infrastructure limits the adoption of this technology despite its critical need.

This chapter concludes that administrative blockchain is not merely a technology but a digital legal guarantee for transparency in crisis management.

Chapter Twenty-Three: Smart Contracts and Cyber Governance of Crises, When Obligations Become Self-Executing Mechanisms

The concept of the administrative contract is no longer confined to paper. It has extended to encompass smart contracts that execute themselves automatically when conditions are met. In times of crises, a smart contract can release aid immediately upon confirmation of the disaster's occurrence through smart sensors.

In practice, some humanitarian organizations have begun using smart contracts. In the International Red Cross, a smart contract is used to release aid immediately upon confirmation of the earthquake's occurrence through satellite data.

In developing nations, the absence of legislation limits the use of these contracts despite their effectiveness.

This chapter affirms that the smart contract is not an alternative to humans but a tool for accelerating justice and response in times of crises.

Chapter Twenty-Four: Vital Data and Cyber Governance of Crises, Protecting Digital Identity of Citizens in Times of Crises

With the increasing use of vital data in crisis management, such as facial recognition and category targeting, a new threat has emerged: the exploitation of digital identity. In some cases, facial recognition algorithms led to the marginalization of racial categories due to data bias.

International law faces absence in protecting vital data. Most legislations do not classify vital data as sensitive data. No international standards exist for collecting vital data in times of crises. Private companies possess biometric records without oversight. In response, some nations have begun establishing controls. In the European Union, the collection of vital data is prohibited without explicit consent. In Canada, the Digital Identity Protection Law criminalizes the use of vital data for discriminatory purposes.

This chapter concludes that vital data must be subject to the principle of maximum protection, because it is part of human dignity.

Chapter Twenty-Five: Artificial Intelligence and Cyber Governance of Crises, Toward Interpretive Algorithms, Explanatory

With the increasing complexity of artificial intelligence algorithms, a fundamental requirement has emerged: the capacity to interpret algorithmic decisions in times of crises. It is not sufficient for the algorithm to say "grant aid to category X." It must explain "why?"

Some nations have developed what is known as interpretive artificial intelligence, which produces decisions that explain their reasons in an understandable manner. In the Netherlands, interpretive algorithms are used for determining evacuation priorities. In Singapore, detailed reports are presented to the judiciary.

In developing nations, the absence of these systems makes algorithmic decisions a black box that cannot be challenged.

This chapter affirms that algorithmic transparency is not a luxury but a fundamental condition for judicial accountability in times of crises.

Chapter Twenty-Six: Adaptive Learning and Cyber Governance of Crises, When Systems Learn from Every Crisis

Fixed digital systems are no longer considered adequate. They have become systems that learn from every crisis to improve their performance in the future. Modern technologies allow algorithms to analyze their errors after every disaster and automatically adjust their behavior.

In practice, some nations have begun applying it. In Japan, adaptive learning systems are used with local earthquake patterns. In Germany, the National Learning Platform analyzes every crisis response to improve future planning.

In developing nations, the absence of historical data limits the effectiveness of these systems.

This chapter concludes that adaptive learning is the heart of cyber governance of crises, because it transforms failure into an opportunity for improvement.

Chapter Twenty-Seven: Cyber Governance of Crises and Augmented Reality, Toward Three-Dimensional Virtual Operations Rooms

Operations rooms are no longer confined to flat screens. They have extended to augmented reality, which displays data in three-dimensional space. In times of crises, decision-makers can visualize the disaster as if they were at its location, with interactive data layers.

In practice, some nations have begun using it. In the United States, augmented reality glasses are used for monitoring forest fires. In South Korea, the Virtual Operations Room allows interaction with a three-dimensional model of the city during crises.

In developing nations, the absence of infrastructure limits the adoption of these technologies.

This chapter affirms that augmented reality is not a toy but a tool for precise decision-making in times of crises.

Chapter Twenty-Eight: Autonomous Robots and Cyber Governance of Crises, When Machines Become First Responders

With the increasing danger of some crises, such as chemical warfare or radiation, the role of autonomous robots has emerged as first responders. These robots do not need humans to operate in lethal environments.

In practice, some nations have begun using them. In Japan, robots are used for exploration after nuclear energy station disasters. In Russia, the Automatic Response Team intervenes in chemical leak cases.

In developing nations, the absence of investment limits the use of these technologies.

This chapter concludes that autonomous robots are not an alternative to humans but a protective shield that preserves human lives in the most dangerous crises.

Chapter Twenty-Nine: Smart Drones and Cyber Governance of Crises, Toward Smart Aerial Surveillance in Real Time

Smart drones are no longer merely imaging tools. They have become smart platforms that analyze data in real time and make immediate decisions. Some drones today are capable of identifying locations of survivors through artificial intelligence and automatically sending their coordinates for rescue.

In practice, some nations have begun using them. In Turkey, smart drones are used for searching for survivors after earthquakes. In Brazil, the Aerial Surveillance Fleet monitors fires and identifies critical ignition points.

In developing nations, the absence of legislation limits the use of these drones effectively.

This chapter affirms that smart drones are the eye of the state in the sky and a necessity in managing modern crises.

Chapter Thirty: The Internet of Things and Cyber Governance of Crises, Toward Smart Infrastructure That Senses Crises Before Their Occurrence

Crises are no longer discovered after their occurrence. They have become sensed through the Internet of Things. Smart sensors distributed in cities, buildings, and bridges send early warnings upon detecting any malfunction.

In practice, some nations have begun applying it. In Singapore, smart sensors are used for predicting landslides. In Italy, the National Internet of Things Network monitors earthquakes before the occurrence of major tremors.

In developing nations, the absence of infrastructure limits the adoption of these networks.

This chapter concludes that the Internet of Things is the nervous system of the modern state and the cornerstone of preventive governance of crises.

Chapter Thirty-One: Cloud Computing and Cyber Governance of Crises, Toward Sovereign Secure Cloud, Administrative

With the increasing dependence on cloud computing, a new threat has emerged: storing crisis data in foreign clouds. In cases of conflict, these services may be cut off or used as tools of pressure.

To confront this threat, some nations have begun creating sovereign clouds. In China, all crisis data is stored in the National Cloud. In Russia, the Yandex Cloud is used exclusively for sensitive data.

In developing nations, the absence of resources pushes them toward dependence on foreign clouds, which exposes them to danger.

This chapter affirms that the sovereign cloud is not a luxury but a fundamental condition for digital sovereignty in times of crises.

Chapter Thirty-Two: Artificial Intelligence and Cyber Governance of Crises, Toward Participatory Systems That Learn from Citizens

Artificial intelligence is no longer confined to relying on official data. It has become interactive with citizens as sources of information. Some systems today analyze social media publications to detect crises before their occurrence.

In practice, some nations have begun using it. In India, artificial intelligence systems analyze citizens' tweets for detecting floods. In Kenya, the Digital Participation Platform allows citizens to report crises through a smart application.

In developing nations, the absence of digital culture limits the effectiveness of these systems.

This chapter concludes that participatory artificial intelligence is a bridge between the state and citizens, and enhances the system's capacity for rapid response.

Chapter Thirty-Three: Open Data and Cyber Governance of Crises, Toward Digital Transparency in Crisis Management

With the increasing demands for transparency, the concept of open data for crises has emerged, which allows citizens to track every stage of response. In some nations, aid distribution data is published in real time through open platforms.

In practice, some nations have begun applying it. In Estonia, all crisis data is published through the Open Data Portal. In Canada, the National Transparency Platform allows citizens to review every administrative decision related to crises.

In developing nations, the absence of legislation limits the adoption of this approach.

This chapter affirms that open data is not a luxury but a tool for societal accountability and against corruption in times of crises.

Chapter Thirty-Four: Artificial Intelligence and Cyber Governance of Crises, Toward Preventive Systems That Prevent Crises Before Their Occurrence

The goal of artificial intelligence is no longer managing crises but preventing them from occurring. Some systems today are capable of analyzing early indicators, such as climate changes or social unrest, and predicting crises months before their occurrence.

In practice, some nations have begun using it. In Germany, preventive systems are used for predicting violent protests. In Japan, the Disaster Prevention Platform analyzes geological data for predicting earthquakes.

In developing nations, the absence of data limits the effectiveness of these systems.

This chapter concludes that preventive artificial intelligence is the peak of the digital pyramid of crises, because it transforms the state from reactive to preventive.

Chapter Thirty-Five: Flexible Legislation and Cyber Governance of Crises, Toward Laws That Adapt to Digital Crises

With the increasing complexity of digital crises, the need has emerged for flexible legislation capable of adapting to new challenges. Some nations today use what is known as dynamic legislation, which is automatically amended based on artificial intelligence recommendations.

In practice, some nations have begun applying it. In Singapore, artificial intelligence systems are used for proposing legislative amendments during crises. In Estonia, Smart Legislation allows amending laws through digital platforms within hours.

In developing nations, legislative bureaucracy limits the flexibility of response.

This chapter affirms that flexible legislation is not chaos but a tool for rapid adaptation to the challenges of the digital age.

Chapter Thirty-Six: Parliamentary Oversight and Cyber Governance of Crises, Toward Smart Oversight of Expenditure in Times of Crises, Digital

Parliamentary oversight is no longer confined to meetings. It has extended to digital oversight platforms that allow tracking every dollar spent in times of crises. Some parliaments today use artificial intelligence systems to detect manipulation in emergency contracts.

In practice, some parliaments have begun using it. In the British Parliament, text analysis systems are used for examining crisis contracts. In the Canadian Parliament, the Smart Oversight Platform allows members to track the flow of funds in real time.

In developing nations, the absence of these systems makes expenditure in times of crises vulnerable to corruption.

This chapter concludes that parliamentary oversight is not an intervention but a guarantee of transparency in the most sensitive times.

Chapter Thirty-Seven: Transitional Justice and Cyber Governance of Crises, Toward Smart Reconciliation After Crises, Digital

Transitional justice is no longer confined to truth and reconciliation. It has extended to digital reconciliation platforms that allow victims to interact in a safe environment. Some systems today use artificial intelligence to analyze victims' testimonies and propose reconciliation solutions.

In practice, some nations have begun using it. In Colombia, digital platforms are used for collecting victims' testimonies. In South Africa, the Smart Reconciliation Platform allows victims to follow the implementation of the Truth Committee's recommendations.

In developing nations, the absence of these platforms makes transitional justice elitist.

This chapter affirms that digital transitional justice is not a luxury but a tool for national healing, and that its absence transforms wounds into permanent scars.

Chapter Thirty-Eight: Digital Education and Cyber Governance of Crises, Toward a Generation Aware of Digital Challenges, Crises

Education about crises is no longer confined to books. It has extended to smart educational platforms that teach crisis management in an interactive manner. Some schools today use virtual reality to simulate disasters and teach students how to respond.

In practice, some nations have begun applying it. In Finland, children learn crisis management through interactive digital games. In Singapore, the Crisis Education Platform allows students to simulate emergency scenarios.

In developing nations, the absence of these platforms makes education a dry experience.

This chapter affirms that digital education for crises is not a luxury but an investment in the future of national security, and that its absence transforms citizens into victims in times of crises.

Chapter Thirty-Nine: Popular Participation and Cyber Governance of Crises, Toward Participatory Democracy in Times of Crises, Digital

The concept of popular participation is no longer confined to elections. It has extended to participatory platforms that allow citizens to contribute to decision-making during crises. Some systems today allow citizens to propose solutions and vote on them in real time.

In practice, some nations have begun using it. In Iceland, citizens are allowed to modify emergency plans through a digital platform. In Taiwan, the Smart Participation Platform allows citizens to propose solutions for crises and modify them.

In developing nations, the absence of these platforms makes popular participation formal.

This chapter affirms that digital popular participation is not a luxury but the essence of democracy in times of crises, and that its absence transforms the state into an entity isolated from its people.

Chapter Forty: Cyber Governance of Crises and the Future, A Strategic Vision for Coming Decades

At the conclusion, cyber governance of crises cannot be viewed as a temporary phenomenon but as a fundamental transformation in the concept of the state in the twenty-first century. Nations that adopt cyber governance of crises today will be capable of: protecting their citizens from digital manipulation in times of crises; building an independent and sustainable digital administrative economy; enhancing the position of their generations in the global administrative system; and participating actively in crafting the rules of the new international order.

Nations that ignore this transformation will find themselves hostage to foreign technology, exposed to external interventions, and incapable of protecting their interests in the digital age. Investment in cyber governance of crises is therefore not a question of choice but a question of survival.

Conclusion

After a comprehensive review of the dimensions of cyber governance of crises across all fields, from cyber security to economy to culture to development, it becomes clear that this concept was never a technical luxury but an existential guarantee for the modern state. The digital administrative space, despite its non-material nature, has become an arena for political and economic conflicts, and no state can maintain its governance of crises without effective national digital capabilities.

This work has revealed that the legislative vacuum constitutes a double threat: it allows major companies and states to impose their dominance, and it leaves developing nations exposed to exploitation without legal protection. To fill this vacuum, a collective initiative is necessary to build a fair international system that balances response efficiency and the right of citizens in digital justice.

In the end, genuine cyber governance of crises is not built on isolation or repression but on transparency, efficiency, and trust between the state and citizens. It is not an end in itself but a means to build a safe administrative future, just and humane.

References

United Nations Office for Disaster Risk Reduction, UNDRR, Global Assessment Report on Disaster Risk Reduction, 2025. International Federation of Red Cross and Red Crescent Societies, IFRC, World Disasters Report, 2024. European Commission, Digital Crisis Management Action Plan, 2024. World Bank, Resilient Infrastructure Guidelines, 2023. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017. General Data Protection Regulation, GDPR, Regulation EU 2016/679. National Institute of Standards and Technology, NIST, Cybersecurity Framework, 2023. Elrakhawi M K A, 2026, The Global Encyclopedia of Law, A Comparative Practical Study, First Edition, Ismailia, Global Legal Publications. Schmitt M N, 2023, Cyber Operations and International Law, Cambridge University Press. Rajamani L, 2025, Crisis Governance and Digital Sovereignty, Oxford University Press. De Schutter O, 2023, The Right to Resilience in the Digital Age, Cambridge University Press. Kloppenburg J R, 2024, Digital Sovereignty and Crisis Exploitation, University of California Press.

Official Government Sources: White House, National Strategy for Digital Crisis Management, 2024. European Commission, Digital Crisis Management Action Plan, 2023. Ministry of Interior Reports on Cyber Resilience in Crisis Systems, Multiple Jurisdictions, 2020 to 2025.

Academic Journals: Journal of International Crisis Law, Oxford. International Journal of Digital Crisis Governance. Harvard Law Review, Crisis Management Section. Stanford Technology Law Review.

Table of Contents

Chapter Six, International Administrative Responsibility for Response Failure, Challenges of Attribution and Oversight. Chapter Seven, Legitimate Responses to Administrative Violations, Between Compensation and Mandatory Acceleration. Chapter Eight, Patents of Invention and Cyber Governance of Crises, The Tension Between Innovation and Administrative Exploitation. Chapter Nine, Cyber Governance of Crises in Developing Nations, Challenges of Capacity and Technological Dependence. Chapter Ten, Regional Organization of Cyber Governance of Crises, A Comparative Study of Global Experiences. Chapter Eleven, National Data and Cyber Governance of Crises, Protecting Administrative Privacy from External Exploitation. Chapter Twelve, Artificial Intelligence and Cyber Governance of Crises, When Algorithms Become Employees, Administrative. Chapter Thirteen, Electronic Crimes and Cyber Governance of Crises, Combating Digital Exploitation in Response, Administrative. Chapter Fourteen, Digital Education and Cyber Governance of Crises, Building Social Awareness as a Foundation for Administrative Defense. Chapter Fifteen, Scientific Research and Cyber Governance of Crises, Toward National Administrative Technological Independence. Chapter Sixteen, Bilateral Agreements and Cyber Governance of Crises, Can Small Nations Protect Themselves. Chapter Seventeen, Courts and Cyber Governance of Crises, Toward Digital Administrative Judicial Jurisdiction. Chapter Eighteen, Administrative Data and Cyber Governance of Crises, Between Individual Ownership and Collective Sovereignty. Chapter Nineteen, Social Justice and Cyber Governance of Crises, Protecting Societies from Irresponsible Administrative Technologies. Chapter Twenty, The Future and Cyber Governance of Crises, Toward a Model International Convention. Chapter Twenty-One, Generative Artificial Intelligence and Cyber Governance of Crises, When Simulation Becomes a Tool for Predicting Crises. Chapter Twenty-Two, Blockchain and Cyber Governance of Crises, Toward Secure and Decentralized Crisis Records, Administrative. Chapter Twenty-Three, Smart Contracts and Cyber Governance of Crises, When Obligations Become Self-Executing Mechanisms. Chapter Twenty-Four, Vital Data and Cyber Governance of Crises, Protecting Digital Identity of Citizens in Times of Crises. Chapter Twenty-Five, Artificial Intelligence and Cyber Governance of Crises, Toward Interpretive Algorithms, Explanatory. Chapter Twenty-Six, Adaptive Learning and Cyber Governance of Crises, When Systems Learn from Every Crisis. Chapter Twenty-Seven, Cyber Governance of Crises and Augmented Reality, Toward Three-Dimensional Virtual Operations Rooms. Chapter Twenty-Eight, Autonomous Robots and Cyber Governance of Crises, When Machines Become First Responders. Chapter Twenty-Nine, Smart Drones and Cyber Governance of Crises, Toward Smart Aerial Surveillance in Real Time. Chapter Thirty, The Internet of Things and Cyber Governance of Crises, Toward Smart Infrastructure That Senses Crises Before Their Occurrence. Chapter Thirty-One, Cloud Computing and Cyber Governance of Crises, Toward Sovereign Secure Cloud, Administrative. Chapter Thirty-Two, Artificial Intelligence and Cyber Governance of Crises, Toward Participatory Systems That Learn from Citizens. Chapter Thirty-Three, Open Data and Cyber Governance of Crises, Toward Digital Transparency in Crisis Management. Chapter Thirty-Four, Artificial Intelligence and Cyber Governance of Crises, Toward Preventive Systems That Prevent Crises Before Their Occurrence. Chapter Thirty-Five, Flexible Legislation and Cyber Governance of Crises, Toward Laws That Adapt to Digital Crises. Chapter Thirty-Six, Parliamentary Oversight and Cyber Governance of Crises, Toward Smart Oversight of Expenditure in Times of Crises, Digital. Chapter Thirty-Seven, Transitional Justice and Cyber Governance of Crises, Toward Smart Reconciliation After Crises, Digital.

Chapter Thirty-Eight, Digital Education and Cyber Governance of Crises, Toward a Generation Aware of Digital Challenges, Crises. Chapter Thirty-Nine, Popular Participation and Cyber Governance of Crises, Toward Participatory Democracy in Times of Crises, Digital. Chapter Forty, Cyber Governance of Crises and the Future, A Strategic Vision for Coming Decades. Conclusion. References. Table of Contents.

Praise be to God, and with Him lies all success.

Authored by Dr. Mohamed Kamal Arafa Elrakhawi.

DOI: 10.5281/zenodo.21806343