

THE EL-RAKHAWI DOCTRINE
CYBER COSMIC WARFARE
TOWARDS DIGITAL SOVEREIGNTY AND THE LAW

OF ARMED CONFLICTS IN THE FIFTH DOMAIN

Author: Dr. Mohamed Kamal Arafa El Rakhawi
International Researcher in Jurisprudence, Philosophy of Law, Cybersecurity, and Cosmic Justice
First Global Academic Edition: September 23, 2026

Digital Object Identifier: 10.5281/zenodo.22909983
Permanent URL: <http://doi.org/10.5281/zenodo.22909983>

Academic Citation:
El Rakhawi, M. K. A. (2026). Cyber Cosmic Warfare: Towards Digital Sovereignty and the Law of Armed Conflicts in the Fifth Domain. The Elrakhawi Doctrine, Volume X. Independent Publication. Zenodo. <http://doi.org/10.5281/zenodo.22909983>

=====

=====

EXECUTIVE SUMMARY

=====

=====

The emergence of cyberspace as a domain of warfare represents the most profound transformation in international security since the advent of nuclear weapons. Unlike traditional domains of land, sea, air, and outer space, cyberspace is borderless, instantaneous, and accessible to state and non-state actors alike. This unique character has created a legal vacuum that threatens to undermine the foundations of international law, state sovereignty, and the protection of civilian populations in the digital age.

This comprehensive volume, the tenth in The Elrakhawi Doctrine series, presents a groundbreaking framework for understanding and governing cyber warfare through the lens of digital sovereignty and the law of armed conflicts. Moving beyond fragmented analyses that treat cyber operations as mere extensions of traditional espionage or criminal activity, this work establishes cyberspace as the fifth sovereign domain, requiring its own comprehensive legal architecture grounded in the principles of sovereignty, proportionality, distinction, and humanity.

The volume is structured around seven integrated pillars. First, the concept of digital sovereignty is established as the foundational principle governing state authority in cyberspace, extending the classical Westphalian framework to the digital realm. Second, the threshold of cyber war is rigorously defined through the Elrakhawi Cyber War Legitimacy Equation (CWLE), a mathematical framework for determining when a cyber operation constitutes an "armed attack"

triggering the right to self-defense under Article 51 of the UN Charter. Third, the operational theaters of cyber warfare are mapped, encompassing critical infrastructure, submarine cables, satellites, sovereign clouds, and digital identity systems. Fourth, the arsenal of weapons of mass digital destruction is analyzed, including autonomous offensive artificial intelligence, ransomware as a state weapon, blockchain warfare, and information manipulation campaigns. Fifth, the rights of victims and mechanisms for compensation are established, recognizing that cyber warfare inflicts harm on individuals, states, corporations, and infrastructure. Sixth, the framework for cyber criminal investigation and digital evidence is developed, addressing the challenges of attribution, chain of custody, and admissibility in judicial proceedings. Seventh, and most innovatively, this volume proposes the supreme judicial architecture for cyber warfare, including the Elrakhawi Universal Declaration on the Prohibition of Autonomous Cyber Weapons, the Geneva Protocols for Cyberspace, and the establishment of an International Court for Cyber War Crimes.

The central thesis of this work is that cyber warfare is not merely a new form of conflict but a qualitative transformation that demands a corresponding transformation in international law. The doctrine of digital sovereignty, first articulated in Volume VII, is here extended and deepened to address the specific challenges of armed conflict in cyberspace. The Elrakhawi Doctrine proposes that every state possesses an inalienable right to digital sovereignty, including the right to control its critical cyber infrastructure, the right to protect its sovereign data, the right to defend against cyber attacks, and the right to participate in the governance of global cyberspace.

This volume draws on comparative analysis of major cyber incidents, including Stuxnet, the Ukraine power grid attacks, SolarWinds, WannaCry, NotPetya, and the Colonial Pipeline ransomware attack, extracting lessons for the development of a comprehensive legal framework. It addresses cutting-edge challenges including the use of artificial intelligence in offensive cyber operations, the weaponization of cryptocurrencies, the manipulation of democratic processes through cyber means, and the emergence of autonomous cyber weapons that can operate without human control.

The Elrakhawi Doctrine on Cyber Cosmic Warfare represents not merely a legal treatise but a philosophical manifesto for the digital age. It calls for a fundamental reimagining of the relationship between state sovereignty and cyberspace, for the establishment of robust safeguards against the weaponization of digital technologies, and for the creation of a global governance architecture that ensures cyberspace serves peace and human flourishing rather than becoming a theater of perpetual conflict. In an era where a single line of code can disable a nation's power grid, steal the identities of millions, or manipulate the outcome of democratic elections, the need for such a framework has never been more urgent.

=====

INTRODUCTION: FROM CYBER CRIME TO COSMIC WAR

=====

=====

The Evolution of Cyber Threats

The history of cyber threats is a history of escalating sophistication, scale, and strategic significance. What began in the 1980s and 1990s as individual acts of hacking and vandalism by hobbyists and activists has evolved into a complex ecosystem of threats encompassing organized crime, state-sponsored espionage, and now full-scale cyber warfare capable of inflicting damage comparable to conventional military operations.

The early period of cyber threats, roughly from 1988 to 2000, was characterized by individual actors motivated by curiosity, notoriety, or ideological causes. The Morris Worm of 1988, which infected approximately 10 percent of the then-connected Internet, demonstrated the potential for widespread disruption but remained an isolated incident rather than a strategic tool.

The period from 2000 to 2010 saw the emergence of cybercrime as a significant economic threat. Organized criminal groups recognized the profit potential of identity theft, financial fraud, and the deployment of malware for extortion. The development of botnets, ransomware, and sophisticated phishing techniques transformed cybercrime into a multi-billion dollar industry that dwarfed the revenues of traditional organized crime.

The period from 2010 to the present has witnessed the weaponization of cyberspace by nation-states. The discovery of Stuxnet in 2010, a sophisticated malware designed to sabotage Iran's nuclear enrichment facilities, marked a watershed moment. For the first time, code had been deployed as a weapon capable of causing physical destruction to critical infrastructure. This was followed by a cascade of state-sponsored cyber operations: the Sony Pictures hack in 2014, the attack on Ukraine's power grid in 2015 and 2016, the WannaCry ransomware attack attributed to North Korea in 2017, the NotPetya attack attributed to Russia in 2017, the SolarWinds supply chain compromise discovered in 2020, and the Colonial Pipeline ransomware attack in 2021.

These incidents demonstrate that cyber operations have evolved from tools of espionage and disruption to instruments of strategic coercion capable of inflicting significant economic, political, and even physical damage. The question is no longer whether cyberspace is a domain of warfare but how international law should regulate this new form of conflict.

Why We Need a New Legal Framework

The existing frameworks of international law, developed primarily in the aftermath of the Second World War and codified in the United Nations Charter, the Geneva Conventions, and customary international law, were designed for a world of physical force, territorial boundaries, and clear distinctions between war and peace. These frameworks, while remarkably resilient and adaptable, face fundamental challenges when applied to cyberspace.

The first challenge is attribution. Unlike a missile strike or a troop invasion, cyber operations can be launched from anywhere in the world, routed through multiple jurisdictions, and designed to obscure their origin. The technical difficulty of attribution, combined with the political incentives for states to deny responsibility, creates a situation where the fundamental principle of state responsibility for internationally wrongful acts is difficult to enforce.

The second challenge is the threshold of force. Traditional international law distinguishes between the use of force (prohibited under Article 2(4) of the UN Charter) and mere frontier incidents or espionage (not prohibited but subject to other legal regimes). Cyber operations often fall into a gray zone: they may cause significant disruption or economic damage without reaching the threshold of physical destruction that would clearly constitute a "use of force" or "armed attack" under traditional interpretations.

The third challenge is the distinction between combatants and civilians. The principles of distinction and proportionality, cornerstone of international humanitarian law, require that attacks be directed only at military objectives and that civilian harm not be excessive in relation to military advantage. In cyberspace, where military and civilian infrastructure are often interconnected and where the effects of cyber operations can cascade unpredictably through networks, applying these principles becomes extraordinarily difficult.

The fourth challenge is the speed and scale of cyber operations. Traditional legal processes for authorizing military action, conducting investigations, and pursuing accountability operate on timescales of days, weeks, or months. Cyber operations can inflict damage in seconds or minutes, creating a temporal mismatch between the speed of attack and the speed of legal response.

The fifth challenge is the role of non-state actors. Traditional international law is primarily concerned with the conduct of states. Cyber warfare, however, involves a complex ecosystem of state actors, state-sponsored groups, independent hackers, criminal organizations, and hacktivists. The legal status and responsibility of these non-state actors in the context of cyber warfare remains poorly defined.

These challenges are not merely technical or legal; they are existential. Without a comprehensive legal framework for cyber warfare, states will continue to operate in a gray zone where aggressive cyber operations carry minimal risk of legal consequences, victims have no effective means of redress, and the potential for escalation into full-scale conflict remains ever-present.

The Methodology of This Work

This volume employs a multi-disciplinary methodology that integrates legal analysis, technical understanding, strategic thinking, and philosophical reflection. The legal analysis draws on the sources of international law enumerated in Article 38 of the Statute of the International Court of

Justice: international conventions, international custom, general principles of law, and judicial decisions and scholarly writings.

The technical understanding is informed by engagement with the cybersecurity community, analysis of malware samples and attack techniques, and consultation with experts in network architecture, cryptography, and digital forensics. This technical grounding is essential for developing legal frameworks that are not merely theoretically sound but practically applicable to the realities of cyber operations.

The strategic thinking is informed by the study of military strategy, deterrence theory, and the history of warfare. Understanding how states think about the use of force, how they calculate risks and benefits, and how they respond to aggression is essential for developing legal frameworks that can effectively regulate state behavior in cyberspace.

The philosophical reflection is informed by the broader themes of The Elrakhawi Doctrine: the nature of sovereignty, the requirements of justice, the protection of human dignity, and the pursuit of peace. These philosophical foundations ensure that the legal frameworks developed are not merely technically competent but morally legitimate.

The structure of this volume follows the classical military planning framework of "when, where, and how," adapted to the specific context of cyber warfare. Part I establishes the foundational concept of digital sovereignty. Part II addresses the threshold question of when cyber operations constitute armed conflict. Part III maps the operational theaters of cyber warfare. Part IV analyzes the arsenal of cyber weapons. Part V addresses the rights of victims. Part VI develops the framework for cyber criminal investigation. Part VII proposes the supreme judicial architecture for cyber warfare.

This structure is not merely organizational; it reflects the logical progression of legal analysis. Before we can regulate cyber warfare, we must establish the foundational principle of digital sovereignty. Before we can apply the law of armed conflict, we must determine when cyber operations cross the threshold of armed conflict. Before we can regulate specific weapons, we must understand the theaters in which they operate. Before we can protect victims, we must understand the nature of the harm they suffer. Before we can prosecute perpetrators, we must develop the investigative and evidentiary frameworks necessary for successful adjudication.

The ultimate goal of this work is not merely to describe the current state of the law but to propose a comprehensive legal architecture for the future. This architecture must be grounded in the fundamental principles of international law while adapted to the unique characteristics of cyberspace. It must be technically feasible while morally legitimate. It must be ambitious in its vision while realistic in its implementation.

The Elrakhawi Doctrine on Cyber Cosmic Warfare represents an attempt to meet this challenge. It is offered not as the final word but as a contribution to an ongoing conversation that must involve states, international organizations, civil society, the technical community, and all those

who recognize that the future of peace and security depends on our ability to bring the rule of law to cyberspace.

=====

=====

PART I: DIGITAL SOVEREIGNTY - THE FIFTH DOMAIN

=====

=====

CHAPTER ONE: CYBERSPACE AS A SOVEREIGN DOMAIN

The Evolution of Sovereignty: From Westphalia to Cyberspace

The concept of sovereignty, in its modern form, emerged from the Peace of Westphalia in 1648, which established the principle that states have exclusive authority over their territory and domestic affairs, free from external interference. This Westphalian framework, while modified and refined over the centuries, remains the foundation of the international legal order.

The Westphalian framework was developed in a world where sovereignty was primarily territorial. A state's authority extended to the land within its borders, the territorial waters adjacent to its coast, and later, the airspace above its territory. The development of international law in the twentieth century extended this framework to outer space, establishing that while outer space is not subject to national appropriation, states retain jurisdiction over their space objects and activities.

Cyberspace presents a fundamental challenge to this territorial conception of sovereignty. Unlike land, sea, air, or outer space, cyberspace is not a physical domain with clear geographical boundaries. It is a virtual domain constituted by networks of interconnected computers, servers, routers, and other devices distributed across the globe. Data flows through this network instantaneously, crossing national borders without regard for territorial boundaries.

This borderless character of cyberspace has led some to argue that the concept of sovereignty is inapplicable to the digital realm. Early cyber-utopians, most famously John Perry Barlow in his 1996 "Declaration of the Independence of Cyberspace," proclaimed that cyberspace is a realm beyond the sovereignty of states, governed not by law but by the collective will of its participants.

This vision, while inspiring, has proven untenable. States have consistently asserted their authority over cyberspace, enacting legislation, establishing regulatory bodies, and conducting cyber operations to protect their interests. The reality is that cyberspace, while borderless in a technical sense, is deeply embedded in the physical world. The infrastructure of cyberspace—servers, routers, fiber optic cables, data centers—is located within the territory of states and subject to their jurisdiction. The users of cyberspace are citizens of states and subject to their

laws. The economic activities conducted in cyberspace generate value that states seek to tax and regulate.

The challenge, therefore, is not whether sovereignty applies to cyberspace but how it applies. The traditional Westphalian framework, developed for a world of physical borders and territorial control, must be adapted to a world where digital activities transcend borders while remaining grounded in physical infrastructure and human communities.

The Four Traditional Domains: Land, Sea, Air, Outer Space

To understand the implications of recognizing cyberspace as a sovereign domain, it is useful to examine how international law has addressed the other domains of human activity.

The domain of land is the most straightforward. State sovereignty over land territory is well-established in international law. A state has exclusive authority over the land within its borders, including the right to control access, regulate activities, and exploit resources. The principle of territorial integrity, enshrined in Article 2(4) of the UN Charter, prohibits the use of force against the territorial integrity or political independence of any state.

The domain of the sea is more complex. The United Nations Convention on the Law of the Sea (UNCLOS) establishes a sophisticated framework that balances the sovereignty of coastal states with the freedom of navigation and other uses of the sea. States have full sovereignty over their internal waters and territorial sea (up to 12 nautical miles from the baseline). They have sovereign rights over the resources of their exclusive economic zone (up to 200 nautical miles) but must respect the freedom of navigation of other states. The high seas are not subject to national appropriation and are open to all states.

The domain of the air was addressed by the Chicago Convention on International Civil Aviation of 1944, which established that states have complete and exclusive sovereignty over the airspace above their territory. This principle is now considered part of customary international law. The boundary between airspace and outer space remains undefined, but the principle of state sovereignty over airspace is well-established.

The domain of outer space was addressed by the Outer Space Treaty of 1967, which established that outer space is not subject to national appropriation and shall be free for exploration and use by all states. However, states retain jurisdiction over their space objects and are responsible for their national space activities, whether conducted by governmental or non-governmental entities.

Each of these domains has required the development of specialized legal frameworks that balance the sovereignty of states with the need for international cooperation and the protection of common interests. Cyberspace will require a similar approach, developing a legal framework that recognizes the sovereign authority of states over their digital infrastructure and activities while establishing rules for international cooperation and the protection of shared interests.

Cyberspace as the Fifth Domain: Characteristics and Challenges

Cyberspace differs from the other four domains in several fundamental ways that create unique challenges for the application of sovereignty.

The first difference is the non-physical nature of cyberspace. Unlike land, sea, air, or outer space, cyberspace is not a physical domain that can be mapped, occupied, or controlled in traditional ways. It is a virtual domain constituted by the interconnection of physical devices through protocols and software. This non-physical character makes it difficult to apply traditional concepts of territorial control and boundary demarcation.

The second difference is the borderless character of cyberspace. Data flows through cyberspace instantaneously, crossing national borders without regard for territorial boundaries. A single transaction may involve servers located in multiple countries, routed through networks controlled by different entities, and affecting users in yet other jurisdictions. This borderless character challenges the traditional conception of sovereignty as territorially bounded authority.

The third difference is the difficulty of attribution. In the physical domains, it is generally possible to identify the source of an action with reasonable certainty. A missile can be traced to its launch site. A ship can be identified by its flag and registration. An aircraft can be tracked by radar. In cyberspace, by contrast, operations can be launched from anywhere in the world, routed through multiple jurisdictions, and designed to obscure their origin. The technical difficulty of attribution, combined with the political incentives for states to deny responsibility, creates a situation where the fundamental principle of state responsibility is difficult to enforce.

The fourth difference is the speed and scale of cyber operations. Physical actions in the traditional domains are constrained by the laws of physics. A missile takes time to reach its target. A ship takes time to traverse the ocean. An aircraft takes time to fly to its destination. Cyber operations, by contrast, can be executed instantaneously and can affect millions of targets simultaneously. This speed and scale create challenges for detection, response, and accountability.

The fifth difference is the role of non-state actors. In the traditional domains, the primary actors are states and their military forces. While non-state actors may operate in these domains (e.g., pirates at sea, terrorists in the air), they are generally marginal compared to state actors. In cyberspace, by contrast, non-state actors play a central role. Criminal organizations, hacktivist groups, independent researchers, and private companies all have significant capabilities and influence. The legal status and responsibility of these non-state actors in the context of cyber operations remains poorly defined.

These differences do not mean that sovereignty is inapplicable to cyberspace. Rather, they mean that the concept of sovereignty must be adapted to the unique characteristics of this domain. The Elrakhawi Doctrine proposes that cyberspace should be recognized as the fifth

sovereign domain, with its own specialized legal framework that builds on the principles of international law while addressing the specific challenges of the digital realm.

Why Existing Legal Frameworks Are Insufficient

The existing frameworks of international law, while remarkably resilient and adaptable, are insufficient to address the challenges of cyberspace for several reasons.

The first reason is the temporal mismatch. International law develops slowly, through the gradual accumulation of state practice and *opinio juris*. The pace of technological change in cyberspace far outstrips the pace of legal development. By the time a legal norm is established, the technology it seeks to regulate may have evolved beyond recognition.

The second reason is the institutional mismatch. The institutions of international law—the United Nations, the International Court of Justice, international tribunals—were designed for a world of physical force and territorial disputes. They lack the technical expertise, the procedural flexibility, and the enforcement mechanisms necessary to address the challenges of cyberspace.

The third reason is the conceptual mismatch. The fundamental concepts of international law—sovereignty, territory, use of force, armed attack—were developed for a world of physical objects and territorial boundaries. Applying these concepts to the virtual realm of cyberspace requires significant adaptation and, in some cases, the development of entirely new concepts.

The fourth reason is the enforcement mismatch. International law relies primarily on state consent and self-help for enforcement. In cyberspace, where attribution is difficult and retaliation may be disproportionate or counterproductive, these traditional enforcement mechanisms are particularly weak.

These mismatches do not mean that international law is irrelevant to cyberspace. The Tallinn Manual 2.0, developed by a group of international legal experts, demonstrates that existing international law can be applied to cyber operations. However, the Tallinn Manual also reveals the gaps and ambiguities in the current legal framework, highlighting the need for further development and clarification.

The Elrakhawi Doctrine proposes that the development of a comprehensive legal framework for cyberspace should proceed on two tracks. The first track is the interpretation and application of existing international law to cyber operations, building on the work of the Tallinn Manual and other scholarly efforts. The second track is the development of new legal norms specifically designed to address the unique challenges of cyberspace, including the recognition of digital sovereignty as a fundamental principle, the establishment of clear thresholds for cyber warfare, and the creation of specialized institutions for adjudication and enforcement.

This dual-track approach ensures that the legal framework for cyberspace is grounded in the established principles of international law while remaining responsive to the unique characteristics of the digital realm. It provides the flexibility necessary to adapt to rapid technological change while maintaining the stability and predictability necessary for effective regulation.

CHAPTER TWO: THE ELRAKHAWI THEORY OF ABSOLUTE DIGITAL SOVEREIGNTY

Defining Digital Sovereignty

Digital sovereignty is the right of a state to exercise exclusive authority over its digital infrastructure, data, and identity systems within its jurisdiction, free from external interference, while respecting the sovereignty of other states and the principles of international law.

This definition encompasses three core elements. The first element is infrastructure sovereignty: the right of a state to control the physical and logical infrastructure of cyberspace within its territory, including servers, routers, fiber optic cables, data centers, and wireless networks. This includes the right to regulate the construction, operation, and security of this infrastructure, to control access to it, and to protect it from external interference or attack.

The second element is data sovereignty: the right of a state to control the data generated, stored, or processed within its jurisdiction, including the right to regulate the collection, use, transfer, and protection of this data. This includes the right to establish data protection standards, to require data localization, and to control cross-border data flows.

The third element is identity sovereignty: the right of a state to control the digital identity systems used within its jurisdiction, including the right to issue digital identities, to authenticate users, and to protect the integrity of identity systems. This includes the right to establish standards for digital identity, to regulate identity providers, and to protect citizens from identity theft and fraud.

These three elements of digital sovereignty are interrelated and mutually reinforcing. Infrastructure sovereignty provides the physical foundation for data and identity sovereignty. Data sovereignty ensures that the information generated within a state's jurisdiction is protected and controlled. Identity sovereignty ensures that the individuals and entities operating within a state's jurisdiction can be authenticated and held accountable.

The Components of Digital Sovereignty

The Elrakhawi Theory of Absolute Digital Sovereignty identifies five components that together constitute the full scope of a state's digital sovereignty.

The first component is critical infrastructure protection. States have the sovereign right and responsibility to protect their critical cyber infrastructure from attack, disruption, or degradation. This includes power grids, water systems, transportation networks, financial systems,

healthcare systems, and communications networks. The protection of critical infrastructure requires a combination of technical measures (firewalls, intrusion detection systems, encryption), organizational measures (incident response plans, security audits, training), and legal measures (regulation, standards, enforcement).

The second component is sovereign data control. States have the sovereign right to control the data generated within their jurisdiction, including the right to regulate its collection, use, storage, and transfer. This includes the right to establish data protection standards, to require data localization for sensitive categories of data, and to control cross-border data flows. The exercise of this right must be balanced against the rights of individuals to privacy and the needs of the global economy for data flows.

The third component is digital identity authentication. States have the sovereign right to establish and maintain digital identity systems that authenticate the identity of individuals and entities operating within their jurisdiction. This includes the right to issue digital identities, to set standards for identity verification, and to regulate identity providers. The exercise of this right must respect the rights of individuals to privacy and to control their own identity.

The fourth component is cyber defense capability. States have the sovereign right to develop and maintain cyber defense capabilities to protect their digital sovereignty from external threats. This includes the right to establish cyber command structures, to train cyber defense personnel, to develop defensive technologies, and to conduct cyber defense operations. The exercise of this right must be consistent with international law, including the principles of necessity, proportionality, and distinction.

The fifth component is international participation. States have the sovereign right to participate in the development of international norms, standards, and institutions for the governance of cyberspace. This includes the right to participate in international negotiations, to propose new norms and standards, and to join international institutions. The exercise of this right must be accompanied by the responsibility to respect the digital sovereignty of other states and to cooperate in addressing shared challenges.

The Relationship Between Digital Sovereignty and Cognitive Sovereignty

The concept of digital sovereignty is closely related to the concept of cognitive sovereignty, first articulated in Volume VII of The Elrakhawi Doctrine. Cognitive sovereignty is the right of individuals to control their own cognitive processes, including their thoughts, beliefs, and decisions, free from external manipulation or control.

Digital sovereignty and cognitive sovereignty are complementary concepts that operate at different levels. Digital sovereignty operates at the level of states, establishing their authority over the digital infrastructure, data, and identity systems within their jurisdiction. Cognitive sovereignty operates at the level of individuals, establishing their right to control their own cognitive processes.

The relationship between these two concepts is symbiotic. Digital sovereignty provides the foundation for cognitive sovereignty by establishing the legal and technical framework within which individuals can exercise control over their digital lives. Without digital sovereignty, states would be unable to protect their citizens from external manipulation, surveillance, or control through digital means.

Conversely, cognitive sovereignty provides the moral foundation for digital sovereignty by establishing that the ultimate purpose of digital sovereignty is to protect the autonomy and dignity of individuals. Without cognitive sovereignty, digital sovereignty could be used as a tool of state control and manipulation rather than as a means of protecting individual rights.

The Elrakhawi Doctrine recognizes that the relationship between digital sovereignty and cognitive sovereignty is not always harmonious. States may invoke digital sovereignty to justify restrictions on individual rights, including freedom of expression, privacy, and access to information. Individuals may invoke cognitive sovereignty to resist state control over their digital lives.

The resolution of these tensions requires a careful balancing of the legitimate interests of states in maintaining order and security with the fundamental rights of individuals to autonomy and dignity. The Elrakhawi Doctrine proposes that this balancing should be guided by the principles of necessity, proportionality, and respect for human dignity, as articulated in international human rights law.

The Limits of Digital Sovereignty: When It Conflicts with Human Rights

The recognition of digital sovereignty as a fundamental principle of international law raises important questions about its limits. When does the exercise of digital sovereignty conflict with the human rights of individuals? When should the international community intervene to protect these rights?

The first limit is the right to privacy. States may invoke digital sovereignty to justify extensive surveillance of their citizens, including the collection of communications data, the monitoring of online activities, and the analysis of behavioral patterns. While states have a legitimate interest in national security and law enforcement, this interest must be balanced against the right to privacy, as recognized in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

The second limit is the right to freedom of expression. States may invoke digital sovereignty to justify restrictions on online speech, including the blocking of websites, the removal of content, and the prosecution of individuals for their online activities. While states may have legitimate reasons for restricting certain categories of speech (e.g., incitement to violence, child pornography), these restrictions must be necessary, proportionate, and prescribed by law, as required by Article 19 of the International Covenant on Civil and Political Rights.

The third limit is the right to access to information. States may invoke digital sovereignty to justify controls on the flow of information across their borders, including the blocking of foreign websites, the filtering of search results, and the requirement that content be localized. While states may have legitimate reasons for regulating information flows (e.g., protecting national security, preventing hate speech), these controls must not unduly restrict the right of individuals to seek, receive, and impart information, as recognized in Article 19 of the International Covenant on Civil and Political Rights.

The fourth limit is the right to participate in public affairs. States may invoke digital sovereignty to justify manipulation of digital platforms, including the use of bots, the amplification of certain voices, and the suppression of others, in order to influence political outcomes. While states have a legitimate interest in maintaining the integrity of their political processes, this interest must not be used as a pretext for manipulating democratic outcomes or suppressing dissent.

The Elrakhawi Doctrine proposes that the exercise of digital sovereignty must be subject to the same human rights standards that apply to the exercise of state authority in other domains. States that violate these standards should be subject to international scrutiny, criticism, and, in extreme cases, sanctions or other forms of international pressure.

The international community has a responsibility to develop mechanisms for monitoring and enforcing compliance with human rights standards in the digital realm. This includes the establishment of independent monitoring bodies, the development of clear standards for state behavior, and the creation of effective remedies for individuals whose rights have been violated.

Towards an International Legal Framework for Digital Sovereignty

The recognition of digital sovereignty as a fundamental principle of international law is only the first step. The next step is the development of a comprehensive international legal framework that specifies the rights and responsibilities of states in the digital realm, establishes mechanisms for cooperation and dispute resolution, and provides for effective enforcement.

The Elrakhawi Doctrine proposes that this framework should be built on five pillars. The first pillar is the recognition of digital sovereignty as a fundamental principle, establishing that states have the right to exercise authority over their digital infrastructure, data, and identity systems while respecting the sovereignty of other states.

The second pillar is the establishment of clear rules of behavior, specifying what states may and may not do in cyberspace, including prohibitions on attacks on critical infrastructure, requirements for due diligence in preventing cyber operations from their territory, and obligations to cooperate in investigating and prosecuting cyber crimes.

The third pillar is the development of confidence-building measures, including transparency mechanisms, notification requirements, and consultation procedures, designed to reduce the risk of misunderstanding and escalation.

The fourth pillar is the creation of institutions for cooperation and dispute resolution, including a standing body for the governance of cyberspace, mechanisms for technical cooperation and capacity building, and procedures for the peaceful resolution of disputes.

The fifth pillar is the establishment of enforcement mechanisms, including the possibility of sanctions for states that violate the rules of behavior, procedures for the attribution of cyber operations to responsible states, and mechanisms for holding individuals accountable for cyber crimes.

This framework is ambitious but necessary. The challenges of cyberspace are too great to be addressed by the existing patchwork of national laws and voluntary norms. Only a comprehensive international legal framework can provide the stability, predictability, and accountability necessary for the peaceful and prosperous development of cyberspace.

The Elrakhawi Doctrine on digital sovereignty represents a contribution to this ongoing effort. It is offered not as a final solution but as a framework for further discussion, negotiation, and development. The ultimate goal is a cyberspace that is secure, stable, open, and free, governed by the rule of law and respectful of human dignity.

CHAPTER THREE: LEGAL CHALLENGES TO DIGITAL SOVEREIGNTY

The Globalization of the Internet vs. National Sovereignty

The tension between the globalization of the Internet and the assertion of national sovereignty is one of the defining challenges of the digital age. The Internet was designed as a borderless network, enabling the free flow of information across national boundaries without regard for territorial jurisdiction. This design reflected the values of the early Internet community, which prioritized openness, decentralization, and individual freedom over state control and territorial authority.

However, as the Internet has grown from a niche academic network to a global infrastructure supporting trillions of dollars in economic activity and billions of daily interactions, states have increasingly asserted their authority over Internet activities within their jurisdiction. This assertion of authority has taken many forms: the enactment of national laws regulating online content, the establishment of national firewalls and filtering systems, the requirement that data be stored locally, and the prosecution of individuals for online activities that violate national laws.

This tension between globalization and sovereignty is not merely technical or legal; it is philosophical and political. It reflects a fundamental disagreement about the nature of

cyberspace and the appropriate role of states in governing it. Some argue that cyberspace is a global commons, akin to the high seas or outer space, that should be governed by international cooperation rather than national authority. Others argue that cyberspace is simply another domain of human activity, subject to the same principles of territorial sovereignty that apply to land, sea, and air.

The reality is more complex. Cyberspace is both global and local, borderless and bounded. The infrastructure of cyberspace is located within the territory of states and subject to their jurisdiction. The users of cyberspace are citizens of states and subject to their laws. But the flows of data and the interactions of users transcend national boundaries, creating challenges for the exercise of territorial authority.

The Elrakhawi Doctrine proposes that this tension should be resolved through a principle of "sovereign interoperability." This principle recognizes that states have the right to regulate Internet activities within their jurisdiction, including the right to establish content standards, data protection rules, and security requirements. However, it also recognizes that the global character of the Internet requires international cooperation and coordination to ensure that these national regulations do not fragment the Internet into isolated national networks.

Sovereign interoperability requires states to exercise their regulatory authority in a manner that is consistent with international law, including the principles of necessity, proportionality, and non-discrimination. It also requires states to cooperate in developing international standards and norms that enable the global Internet to function while respecting the legitimate regulatory interests of individual states.

The Role of Multinational Corporations

The governance of cyberspace is not solely a matter of state authority. Multinational corporations, particularly the major technology companies—Google, Meta (Facebook), Amazon, Apple, Microsoft—play a central role in shaping the digital environment. These companies control the platforms through which billions of people communicate, access information, and conduct business. They establish the terms of service that govern user behavior, the algorithms that determine what content is visible, and the technical standards that enable interoperability.

The power of these corporations raises fundamental questions about accountability and legitimacy. Unlike states, which are subject to democratic oversight and international law, these corporations are private entities accountable primarily to their shareholders. Their decisions about content moderation, data collection, and algorithmic design affect billions of people but are made without public input or democratic legitimacy.

The Elrakhawi Doctrine proposes that the role of multinational corporations in the governance of cyberspace should be subject to international standards and oversight. These standards should address issues such as transparency in content moderation, protection of user privacy,

accountability for algorithmic decisions, and cooperation with law enforcement and national security authorities.

The development of these standards requires cooperation between states, international organizations, civil society, and the private sector. It also requires the development of new institutional mechanisms for oversight and accountability, including independent monitoring bodies, multi-stakeholder governance structures, and effective remedies for individuals whose rights have been violated by corporate actions.

The Chinese Challenge: Sovereign Internet vs. Open Internet

The approach of the People's Republic of China to Internet governance represents a fundamental challenge to the Western conception of an open and free Internet. China has developed a sophisticated system of Internet control, often referred to as the "Great Firewall," which blocks access to foreign websites, filters content, monitors online activities, and requires real-name registration for Internet users.

The Chinese model is based on the principle of "cyber sovereignty," which asserts that states have the right to control Internet activities within their jurisdiction without external interference. This principle has gained traction in international forums, particularly among states that are skeptical of the Western-dominated model of Internet governance.

The Chinese model raises fundamental questions about the relationship between sovereignty and human rights. While states clearly have the right to regulate Internet activities within their jurisdiction, this right is not unlimited. It must be exercised in a manner consistent with international human rights standards, including the rights to freedom of expression, privacy, and access to information.

The Elrakhawi Doctrine recognizes the legitimate interest of states in maintaining order and security in cyberspace. However, it also affirms that the exercise of digital sovereignty must respect fundamental human rights. States that use digital sovereignty as a pretext for suppressing dissent, controlling information, or violating the rights of their citizens should be subject to international scrutiny and pressure.

The international community should engage with China and other states that assert strong control over their digital environments, seeking to promote respect for human rights while acknowledging the legitimate security concerns of these states. This engagement should be based on dialogue, cooperation, and the development of shared norms and standards that balance sovereignty with human rights.

Towards an International Legal Framework for Digital Sovereignty

The challenges to digital sovereignty—globalization, corporate power, and divergent national models—demonstrate the need for a comprehensive international legal framework that can

reconcile these competing interests and provide a stable foundation for the governance of cyberspace.

The Elrakhawi Doctrine proposes that this framework should be built on the following principles:

The principle of sovereign equality: All states have equal sovereignty over their digital environments, regardless of their size, wealth, or technological capability. No state should be able to impose its will on other states through cyber operations or other forms of coercion.

The principle of non-intervention: States should not interfere in the digital affairs of other states, including through cyber operations designed to disrupt, degrade, or manipulate the digital infrastructure, data, or identity systems of other states.

The principle of due diligence: States should take reasonable measures to prevent their territory from being used for cyber operations that harm other states. This includes enacting and enforcing laws against cyber crime, cooperating in investigations, and taking action against non-state actors operating from their territory.

The principle of cooperation: States should cooperate in addressing shared challenges in cyberspace, including cyber crime, cyber terrorism, and threats to critical infrastructure. This cooperation should be based on mutual respect, reciprocity, and shared responsibility.

The principle of human rights: The exercise of digital sovereignty must respect fundamental human rights, including the rights to freedom of expression, privacy, and access to information. States that violate these rights should be subject to international scrutiny and pressure.

The principle of accountability: States and non-state actors should be held accountable for their actions in cyberspace. This includes the attribution of cyber operations to responsible states, the prosecution of individuals for cyber crimes, and the provision of remedies for victims of cyber operations.

These principles provide a foundation for the development of a comprehensive international legal framework for digital sovereignty. They are not exhaustive, and they will require further elaboration and refinement through international negotiation and practice. However, they represent a starting point for the difficult but necessary task of bringing the rule of law to cyberspace.

The Elrakhawi Doctrine on digital sovereignty is offered as a contribution to this ongoing effort. It recognizes the complexity of the challenges and the diversity of interests at stake. It seeks to balance the legitimate authority of states with the fundamental rights of individuals and the need for international cooperation. It is ambitious but realistic, grounded in the principles of international law while responsive to the unique characteristics of cyberspace.

The ultimate goal is a cyberspace that is secure, stable, open, and free, governed by the rule of law and respectful of human dignity. This goal will not be achieved easily or quickly. It will require sustained effort, political will, and international cooperation. But it is a goal worth pursuing, for the future of peace, security, and prosperity depends on our ability to bring the rule of law to the digital realm.

=====

THE ELRAKHAWI DOCTRINE: VOLUME X (PART 2 OF 3)
CYBER COSMIC WARFARE
TOWARDS DIGITAL SOVEREIGNTY AND THE LAW OF ARMED CONFLICTS IN THE FIFTH
DOMAIN

=====

PART II: WHEN - THE THRESHOLD OF CYBER WAR

=====

CHAPTER FOUR: THE ELRAKHAWI CYBER WAR LEGITIMACY EQUATION (CWLE)

The Need for a Mathematical Framework

The determination of when a cyber operation constitutes an "armed attack" triggering the right to self-defense under Article 51 of the UN Charter has been one of the most contentious issues in international cyber law. Traditional legal analysis relies on qualitative assessments of scale, effects, and intent, leading to inconsistent conclusions and strategic ambiguity. The Elrakhawi Doctrine proposes a quantitative approach through the Cyber War Legitimacy Equation (CWLE), a mathematical framework that provides objective criteria for threshold determination.

The CWLE is grounded in the recognition that cyber operations exist on a spectrum from mere nuisance to full-scale warfare, and that the threshold of armed conflict should be determined by the cumulative weight of multiple factors rather than any single criterion. This approach draws on the "scale and effects" test articulated by the International Court of Justice in the Nicaragua case while adapting it to the unique characteristics of cyber operations.

The Components of the CWLE

The CWLE is expressed as a composite index that integrates four critical dimensions of cyber operations:

$$CWLE = (S_e \times I_n \times P_r) / (D_c \times C_v)$$

Where the numerator represents factors that increase the likelihood of threshold crossing:

S_e (Scale of Effects): A quantitative measure of the physical, economic, and social consequences of the cyber operation. This includes direct financial losses, disruption of critical services, physical damage to infrastructure, and casualties (injuries or deaths). The scale is measured on a logarithmic scale from 0.1 (minimal disruption) to 10.0 (catastrophic consequences comparable to conventional military attack).

I_n (Intent and Attribution Confidence): A measure of the confidence level in attributing the operation to a state actor and the clarity of hostile intent. This ranges from 0.1 (uncertain attribution, ambiguous intent) to 10.0 (clear state attribution, explicit hostile declaration). The attribution confidence is based on technical indicators, intelligence assessments, and pattern analysis.

P_r (Proportionality to Political Objectives): A measure of whether the cyber operation is proportionate to the political objectives it seeks to achieve. Disproportionate attacks that cause excessive harm relative to their strategic purpose are more likely to cross the threshold. This ranges from 0.1 (highly disproportionate) to 10.0 (strictly proportionate to legitimate military objectives).

Where the denominator represents factors that mitigate threshold crossing:

D_c (Dual-Use Character): A measure of the extent to which the targeted infrastructure or systems serve both civilian and military purposes. Attacks on purely military targets are more likely to cross the threshold than attacks on dual-use infrastructure. This ranges from 0.1 (purely civilian target) to 10.0 (exclusively military target).

C_v (Civilian Vulnerability): A measure of the vulnerability of civilian populations to the consequences of the cyber operation. Operations that disproportionately affect civilians are less likely to be considered legitimate acts of war and more likely to be considered war crimes. This ranges from 0.1 (minimal civilian impact) to 10.0 (severe civilian harm).

Interpreting the CWLE Score

The CWLE produces a composite score that indicates the likelihood that a cyber operation has crossed the threshold of armed conflict:

A CWLE score above 7.0 indicates a high probability that the operation constitutes an armed attack, triggering the right to self-defense under Article 51. This typically involves operations with severe physical consequences, clear state attribution, and disproportionate effects.

A CWLE score between 4.0 and 7.0 indicates a gray zone where the operation may constitute a use of force but not necessarily an armed attack. These operations may justify countermeasures but not military self-defense.

A CWLE score below 4.0 indicates that the operation falls below the threshold of armed conflict, constituting either a mere frontier incident, espionage, or criminal activity. These operations should be addressed through law enforcement, diplomatic channels, or economic countermeasures rather than military response.

Application of the CWLE to Historical Cases

To validate the CWLE, it is instructive to apply it to major cyber incidents and assess whether the scores align with legal and policy responses.

The Stuxnet operation (2010), which caused physical damage to Iran's nuclear centrifuges, would score approximately 8.5 on the CWLE. The scale of effects was significant (physical destruction of critical infrastructure), attribution confidence was high (widely attributed to the United States and Israel), the operation was proportionate to the objective of preventing nuclear proliferation, the target was primarily military/nuclear in character, and civilian vulnerability was relatively low. This score aligns with the widespread view that Stuxnet constituted a use of force, though debate continues over whether it reached the threshold of armed attack.

The Ukraine power grid attacks (2015, 2016), which caused temporary blackouts affecting hundreds of thousands of civilians, would score approximately 5.5. The scale of effects was moderate (temporary disruption without permanent damage), attribution confidence was high (attributed to Russian military intelligence), the operation was disproportionate to any legitimate military objective, the target was dual-use (civilian power infrastructure), and civilian vulnerability was high. This score reflects the ambiguous legal status of these operations, which most states considered unacceptable but stopped short of characterizing as armed attacks.

The WannaCry ransomware attack (2017), which affected hundreds of thousands of computers worldwide including healthcare systems, would score approximately 3.5. The scale of effects was significant in aggregate but diffuse, attribution confidence was moderate (attributed to North Korea but with lower confidence than state-sponsored military operations), the operation was highly disproportionate (indiscriminate attack affecting civilians globally), the target was predominantly civilian, and civilian vulnerability was extremely high. This score aligns with the characterization of WannaCry as a criminal act rather than an act of war, though it may constitute a violation of international law if state-sponsored.

The SolarWinds supply chain compromise (2020), which enabled espionage against thousands of organizations including US government agencies, would score approximately 2.0. The scale of effects was primarily informational (espionage rather than destruction), attribution confidence was high (attributed to Russian intelligence), the operation was proportionate to intelligence-gathering objectives, the target was government/military systems, and civilian vulnerability was low. This score reflects the consensus that SolarWinds constituted espionage rather than armed conflict, though it violated international norms.

Limitations and Refinements of the CWLE

The CWLE provides a valuable quantitative framework for threshold determination, but it has limitations that must be acknowledged. First, the assignment of numerical values to qualitative factors involves subjective judgment and may vary between analysts. Second, the equation assumes that the factors are independent and additive, whereas in reality they may interact in complex ways. Third, the CWLE does not account for cumulative effects of multiple cyber operations over time, which may collectively cross the threshold even if individual operations do not.

To address these limitations, the Elrakhawi Doctrine proposes several refinements. First, the assignment of values should be conducted by independent panels of technical and legal experts using standardized methodologies. Second, sensitivity analysis should be conducted to assess how variations in input values affect the output score. Third, a cumulative effects modifier should be added to account for patterns of cyber operations that collectively constitute armed conflict.

The CWLE is not intended to replace legal judgment but to inform it. The ultimate determination of whether a cyber operation constitutes an armed attack remains a legal question that must be answered by states and international tribunals. However, the CWLE provides a structured, transparent, and replicable framework for making these determinations, reducing ambiguity and enhancing accountability.

CHAPTER FIVE: WHEN DOES A CYBER ATTACK CONSTITUTE AN ARMED ATTACK?

Article 51 of the UN Charter and the Right to Self-Defense

Article 51 of the United Nations Charter establishes the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. This provision is the cornerstone of the international legal framework governing the use of force, and its application to cyber operations is one of the most critical questions in contemporary international law.

The traditional interpretation of "armed attack" under Article 51 requires that the attack involve the use of armed force causing significant physical damage or casualties. This interpretation is grounded in the text of the Charter, which refers to "armed force" in Article 2(4) and "armed attack" in Article 51, suggesting that the drafters contemplated kinetic military operations rather than other forms of coercion.

However, the International Court of Justice has recognized that the concept of armed attack is not limited to operations involving armed forces. In the Nicaragua case, the Court distinguished between "the most grave forms of the use of force" (constituting armed attack) from "other less grave forms" (constituting mere use of force). This distinction suggests that the threshold of armed attack is determined by the gravity of the consequences rather than the means employed.

The application of this reasoning to cyberspace raises the question of whether cyber operations can constitute armed attacks even in the absence of kinetic force. The Elrakhawi Doctrine argues that they can, provided that the consequences are sufficiently grave. A cyber operation that causes widespread death, destroys critical infrastructure, or inflicts economic damage comparable to a conventional military attack should be considered an armed attack regardless of the means employed.

The Threshold of "Use of Force" vs. "Armed Attack"

International law distinguishes between the "use of force" prohibited under Article 2(4) of the UN Charter and the "armed attack" that triggers the right to self-defense under Article 51. All armed attacks are uses of force, but not all uses of force are armed attacks. This distinction creates a gap in which states may engage in coercive cyber operations that violate Article 2(4) but do not justify military self-defense under Article 51.

The threshold between use of force and armed attack is not precisely defined in international law. The Tallinn Manual 2.0 suggests that the determination should be based on the "scale and effects" of the operation, considering factors such as the severity of consequences, the immediacy of effects, the directness of impact, the measurability of effects, the presumptive legitimacy of the target, the extent of intrusion into the target state, and the involvement of the state in the operation.

The Elrakhawi Doctrine proposes that this threshold should be determined through the CWLE framework, which provides a more structured and transparent approach than the multi-factor test of the Tallinn Manual. Under the CWLE, cyber operations scoring above 7.0 should be considered armed attacks, those scoring between 4.0 and 7.0 should be considered uses of force justifying countermeasures but not self-defense, and those scoring below 4.0 should be considered below the threshold of Article 2(4).

Case Studies: When Cyber Operations Cross the Threshold

To illustrate the application of these principles, it is instructive to examine specific cases where cyber operations have raised questions about threshold crossing.

The 2007 cyber attacks on Estonia, which disrupted government websites, banks, and media outlets for several weeks, are widely considered to have fallen below the threshold of armed attack. While the attacks caused significant disruption and economic damage, they did not result in physical destruction or casualties. Most legal scholars characterize these attacks as mere uses of force or even below the threshold of Article 2(4), constituting criminal activity rather than international wrongful acts by a state.

The 2008 cyber attacks on Georgia, which accompanied the Russian military invasion, are more ambiguous. While the cyber operations themselves did not cause significant physical damage,

they were coordinated with kinetic military operations and may have facilitated the invasion by disrupting Georgian communications and command systems. In this context, the cyber operations may be considered part of a broader armed attack, even if they would not independently cross the threshold.

The 2014 Sony Pictures hack, attributed to North Korea in retaliation for the film "The Interview," caused significant economic damage and embarrassment but did not result in physical destruction or casualties. Most legal scholars characterize this as a criminal act or possibly a use of force, but not an armed attack justifying military self-defense. The appropriate response would be law enforcement cooperation, economic sanctions, or diplomatic measures rather than military action.

The 2021 Colonial Pipeline ransomware attack, while attributed to a criminal group rather than a state, demonstrated the potential for cyber operations to cause significant economic disruption and even physical consequences (gasoline shortages in the southeastern United States). If this attack had been state-sponsored and directed at critical infrastructure with the intent to cause severe economic harm, it might have approached the threshold of armed attack under the CWLE framework.

The Right to Self-Defense in Cyberspace

When a cyber operation constitutes an armed attack, the victim state has the right to respond in self-defense under Article 51. This right is subject to the conditions of necessity and proportionality established in customary international law and articulated in the Caroline case.

The condition of necessity requires that the response be necessary to repel the armed attack and that no peaceful means of resolution are available. In the cyber context, this may be difficult to satisfy given the availability of diplomatic, economic, and law enforcement measures. However, if the armed attack is ongoing or if peaceful means have been exhausted or are clearly futile, the condition of necessity may be satisfied.

The condition of proportionality requires that the response be proportionate to the armed attack it seeks to repel. This does not mean that the response must be identical in kind or scale, but that it must not be excessive in relation to the legitimate objective of repelling the attack. In the cyber context, this raises the question of whether a state may respond to a cyber armed attack with kinetic military force, or whether the response must also be in cyberspace.

The Elrakhawi Doctrine argues that the response need not be in the same domain as the attack. A state that suffers a cyber armed attack may respond with kinetic military force if such response is necessary and proportionate to repel the attack. However, the response should generally be in cyberspace unless the cyber attack has caused physical damage or casualties that justify a kinetic response.

The doctrine also recognizes the right to collective self-defense, allowing states to come to the aid of allies that have suffered cyber armed attacks. This right is particularly important in cyberspace, where individual states may lack the technical capacity to respond effectively to sophisticated cyber operations. Collective self-defense enables pooling of capabilities and coordinated response, enhancing deterrence and resilience.

CHAPTER SIX: LAWFUL CYBER RESPONSE AND DETERRENCE

The Principle of Proportionality in Cyber Response

The principle of proportionality is a cornerstone of the law of self-defense, requiring that any response to an armed attack be proportionate to the attack itself. In the cyber context, proportionality raises complex questions about the relationship between cyber and kinetic responses, the measurement of harm, and the temporal dimension of response.

The Elrakhawi Doctrine proposes that proportionality in cyber response should be assessed through a multi-dimensional framework that considers not only the immediate effects of the attack but also its long-term consequences, its strategic context, and the legitimate objectives of the response. A response that causes greater immediate harm than the attack may still be proportionate if it is necessary to prevent future attacks or to restore the strategic balance.

However, the doctrine also recognizes limits on proportionality. Responses that cause excessive civilian harm, that target purely civilian infrastructure, or that violate other principles of international humanitarian law are disproportionate regardless of the severity of the initial attack. The doctrine calls for the development of clear guidelines on proportionality in cyber response, drawing on the principles of international humanitarian law and adapted to the unique characteristics of cyberspace.

Cyber Response vs. Traditional Military Response

The question of whether a state may respond to a cyber armed attack with traditional military force is one of the most contentious issues in international cyber law. Some scholars argue that the response must be in the same domain as the attack, while others argue that the response may be in any domain provided it is necessary and proportionate.

The Elrakhawi Doctrine takes the position that the response need not be in the same domain. The right to self-defense under Article 51 is not limited to responses in the same domain as the attack. A state that suffers a cyber armed attack may respond with kinetic military force if such response is necessary and proportionate to repel the attack and prevent future attacks.

However, the doctrine recognizes that kinetic responses to cyber attacks raise significant escalation risks and may be disproportionate in many cases. The doctrine therefore establishes a presumption in favor of cyber responses, with kinetic responses justified only in cases where the cyber attack has caused physical damage or casualties, where cyber response capabilities

are insufficient, or where the attacking state has demonstrated a pattern of escalating cyber aggression that can only be deterred through kinetic means.

The doctrine also recognizes the right to respond with economic measures, diplomatic sanctions, or law enforcement cooperation. These measures may be more appropriate than military response in cases where the cyber attack does not reach the threshold of armed attack but nevertheless violates international law or norms.

Cyber Deterrence: Theory and Practice

Deterrence is the prevention of adversary action through the threat of unacceptable consequences. In the cyber context, deterrence is particularly challenging due to the difficulties of attribution, the asymmetry between attackers and defenders, the involvement of non-state actors, and the speed and scale of cyber operations.

The Elrakhawi Doctrine proposes a comprehensive approach to cyber deterrence that combines punishment, denial, and entanglement strategies. Punishment deterrence threatens unacceptable consequences for cyber aggression, including military response, economic sanctions, or cyber counter-attacks. Denial deterrence reduces the likelihood of successful attacks through robust defense, resilience, and redundancy. Entanglement deterrence increases the costs of cyber aggression by creating mutual dependencies that make attacks self-defeating.

The doctrine recognizes that no single deterrence strategy is sufficient. Effective cyber deterrence requires a combination of all three strategies, tailored to the specific threat and context. Punishment deterrence is most effective against state actors with valuable assets at risk. Denial deterrence is most effective against criminal actors seeking easy targets. Entanglement deterrence is most effective in contexts of mutual economic or technological dependence.

The doctrine also recognizes the importance of signaling and communication in deterrence. Adversaries must understand the consequences of cyber aggression and the thresholds that will trigger response. The doctrine calls for the development of clear red lines, communicated through diplomatic channels and public statements, that establish the conditions under which cyber operations will be considered armed attacks justifying military response.

The Role of International Alliances in Collective Deterrence

Individual states may lack the technical capacity or strategic leverage to deter sophisticated cyber aggression alone. International alliances and partnerships are therefore essential for effective cyber deterrence. NATO, the European Union, and other regional organizations have recognized cyber defense as a core mission and have developed frameworks for collective response to cyber attacks.

The Elrakhawi Doctrine advocates for the strengthening of collective cyber deterrence through formal alliances, information sharing, joint exercises, and coordinated response capabilities. The doctrine proposes the establishment of a Cyber Defense Coalition, analogous to NATO's collective defense commitment under Article 5, under which an armed attack against one member in cyberspace would be considered an attack against all members.

The doctrine also recognizes the importance of public-private partnerships in cyber deterrence. Private companies control much of the critical infrastructure and possess technical capabilities that states lack. Effective deterrence requires cooperation between governments and private sector entities, including information sharing, joint threat assessment, and coordinated response.

However, the doctrine also recognizes the risks of alliance-based deterrence, including escalation risks, the potential for misattribution leading to collective response against innocent parties, and the challenge of maintaining alliance cohesion in the face of divergent national interests. The doctrine calls for careful calibration of collective deterrence commitments, with clear procedures for attribution, decision-making, and response to ensure that collective action is legitimate, proportionate, and effective.

=====

=====

PART III: WHERE - THE OPERATIONAL THEATERS OF CYBER WARFARE

=====

=====

CHAPTER SEVEN: CRITICAL INFRASTRUCTURE

Defining Critical Infrastructure in the Digital Age

Critical infrastructure refers to the physical and virtual systems and assets that are so vital to a nation that their incapacity or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. In the digital age, critical infrastructure encompasses not only traditional physical systems such as power grids, water treatment facilities, and transportation networks, but also the digital systems that control, monitor, and optimize these physical systems.

The convergence of operational technology (OT) and information technology (IT) has created new vulnerabilities in critical infrastructure. Historically, OT systems controlling industrial processes were isolated from IT networks and the Internet, providing a degree of security through obscurity. However, the drive for efficiency, remote monitoring, and integration with enterprise systems has connected OT systems to IT networks and, in many cases, to the Internet, exposing them to cyber threats.

The Elrakhawi Doctrine recognizes that critical infrastructure is the primary target of cyber warfare due to its strategic importance and the cascading effects of its disruption. An attack on a power grid can disable communications, transportation, healthcare, and financial systems. An attack on a water treatment facility can cause public health crises. An attack on transportation networks can paralyze economic activity and emergency response.

Sectors of Critical Infrastructure

The doctrine identifies eight sectors of critical infrastructure that are particularly vulnerable to cyber attack and particularly important for national security and public welfare:

The energy sector includes power generation, transmission, and distribution systems, as well as oil and gas production, refining, and distribution. Cyber attacks on this sector can cause widespread blackouts, fuel shortages, and economic disruption. The 2015 and 2016 attacks on Ukraine's power grid demonstrated the potential for cyber operations to cause physical disruption to energy infrastructure.

The water sector includes water treatment, distribution, and wastewater systems. Cyber attacks on this sector can contaminate water supplies, disable treatment processes, or cause flooding through manipulation of control systems. The 2021 attempt to poison the water supply in Oldsmar, Florida, demonstrated the vulnerability of water systems to cyber attack.

The transportation sector includes aviation, maritime, rail, and road transportation systems. Cyber attacks on this sector can disrupt logistics, cause accidents, or paralyze economic activity. The potential for cyber attacks to affect aircraft navigation systems or train control systems raises particular safety concerns.

The healthcare sector includes hospitals, clinics, pharmaceutical manufacturers, and public health systems. Cyber attacks on this sector can disrupt patient care, compromise medical records, or disable critical medical equipment. The WannaCry attack on the UK's National Health Service in 2017 demonstrated the potential for ransomware to cause harm to patients by disrupting healthcare delivery.

The financial sector includes banks, stock exchanges, payment systems, and insurance companies. Cyber attacks on this sector can cause economic disruption, steal funds, or undermine confidence in financial institutions. The 2016 Bangladesh Bank heist, in which hackers attempted to steal nearly \$1 billion, demonstrated the potential for cyber attacks to cause significant financial losses.

The communications sector includes telecommunications networks, Internet service providers, and satellite communications. Cyber attacks on this sector can disrupt communications, enable surveillance, or facilitate other attacks by disabling the infrastructure needed for coordination and response.

The government sector includes federal, state, and local government systems, including those responsible for national security, law enforcement, and public services. Cyber attacks on this sector can compromise sensitive information, disrupt government operations, or undermine public confidence in government institutions.

The defense sector includes military command and control systems, weapons systems, and intelligence systems. Cyber attacks on this sector can compromise military operations, disable weapons systems, or steal classified information. This sector is likely to be a primary target in any major cyber conflict between states.

Protecting Critical Infrastructure: Legal and Technical Frameworks

The protection of critical infrastructure requires a combination of legal, technical, and organizational measures. The Elrakhawi Doctrine proposes a comprehensive framework for critical infrastructure protection that addresses all three dimensions.

The legal framework should establish clear obligations for critical infrastructure operators to implement cybersecurity measures, report incidents, and cooperate with government authorities. The framework should also establish liability for failures to protect critical infrastructure that result in harm to public safety or national security. The doctrine calls for the development of international standards for critical infrastructure protection, recognizing that cyber threats transcend national boundaries and require coordinated international response.

The technical framework should include requirements for network segmentation, access controls, encryption, intrusion detection, and incident response capabilities. The doctrine recognizes that no technical measure can provide absolute security, but that layered defense can significantly reduce the likelihood and impact of successful attacks. The doctrine also calls for investment in research and development of advanced cybersecurity technologies, including artificial intelligence for threat detection and response.

The organizational framework should include clear assignment of responsibilities, regular training and exercises, information sharing mechanisms, and coordination between government and private sector entities. The doctrine recognizes that critical infrastructure is largely owned and operated by private companies, and that effective protection requires close cooperation between government and industry.

Case Studies: Attacks on Critical Infrastructure

To illustrate the vulnerabilities and consequences of cyber attacks on critical infrastructure, it is instructive to examine specific cases.

The 2015 attack on Ukraine's power grid, attributed to Russian military intelligence, used malware to disrupt the control systems of three energy distribution companies, causing blackouts affecting approximately 230,000 customers. The attack demonstrated the feasibility of

cyber operations to cause physical disruption to critical infrastructure and the potential for cascading effects on other systems dependent on electricity.

The 2017 WannaCry ransomware attack affected hundreds of thousands of computers worldwide, including many in the UK's National Health Service. The attack encrypted medical records and disabled computer systems, forcing hospitals to cancel appointments and divert ambulances. While no deaths were directly attributed to the attack, the disruption to healthcare delivery likely caused harm to patients.

The 2021 Colonial Pipeline ransomware attack, attributed to the DarkSide criminal group, forced the company to shut down the largest fuel pipeline in the United States, causing gasoline shortages and panic buying in the southeastern states. The attack demonstrated the vulnerability of critical infrastructure to ransomware and the potential for criminal actors to cause significant economic and social disruption.

The 2021 attempt to poison the water supply in Oldsmar, Florida, involved an unauthorized remote access to the water treatment facility's control system and an attempt to increase the level of lye in the water to dangerous levels. The attack was detected and prevented by an operator, but it demonstrated the vulnerability of water treatment systems to cyber attack and the potential for cyber operations to cause direct harm to public health.

These cases demonstrate the urgent need for comprehensive critical infrastructure protection and the potential consequences of failure. The Elrakhawi Doctrine calls for sustained investment in critical infrastructure cybersecurity, international cooperation on standards and best practices, and clear legal frameworks establishing responsibilities and accountability.

CHAPTER EIGHT: SUBMARINE CABLES AND SATELLITES

Submarine Cables: The Arteries of the Global Internet

Submarine communications cables are the backbone of the global Internet, carrying approximately 95 percent of intercontinental data traffic. These cables, lying on the ocean floor, connect continents and enable the global flow of information, commerce, and communication. The vulnerability of these cables to physical and cyber attack represents a significant strategic risk.

The physical vulnerability of submarine cables has been recognized for decades. Cables can be damaged by fishing activities, ship anchors, natural disasters, or deliberate sabotage. The redundancy of the cable network provides some resilience, as traffic can be rerouted through alternative paths if a cable is damaged. However, certain chokepoints where multiple cables converge are particularly vulnerable, and the loss of multiple cables in a region could cause significant disruption.

The cyber vulnerability of submarine cables is less well understood but potentially more significant. The landing stations where cables come ashore contain sophisticated equipment for signal processing and routing. These stations are connected to terrestrial networks and may be vulnerable to cyber attack. An attack on a landing station could disrupt not only the cable it serves but also the terrestrial networks it connects to, causing cascading effects.

The Elrakhawi Doctrine recognizes that submarine cables are critical infrastructure of strategic importance and calls for their protection under international law. The doctrine proposes that attacks on submarine cables, whether physical or cyber, should be considered violations of international law and, if sufficiently severe, may constitute armed attacks justifying self-defense.

Attacks on Submarine Cables: Threats and Protection

The threats to submarine cables range from accidental damage to deliberate attack. Accidental damage from fishing activities or ship anchors is relatively common and is addressed through cable burial, marking, and international cooperation on cable protection zones. Deliberate attack is less common but more serious, raising questions about attribution, responsibility, and response.

The physical cutting of submarine cables has occurred in several instances, most notably the 2008 disruption of multiple cables in the Mediterranean and the Red Sea that affected Internet connectivity in the Middle East and South Asia. While these disruptions were attributed to accidental causes or ship anchors, they demonstrated the vulnerability of the cable network and the potential for cascading effects.

The possibility of deliberate attack on submarine cables by state actors is a growing concern. Submarines equipped with specialized equipment could physically cut cables, or cyber attacks could disrupt landing stations or the cables themselves through manipulation of control systems. The strategic impact of such attacks could be significant, disrupting communications, commerce, and military operations.

The Elrakhawi Doctrine calls for the development of international norms and legal frameworks for the protection of submarine cables. The doctrine proposes that states should be prohibited from deliberately attacking submarine cables except in the context of armed conflict and in accordance with the principles of international humanitarian law. The doctrine also calls for the development of technical measures to enhance the resilience of the cable network, including redundancy, monitoring, and rapid repair capabilities.

Satellites: The Orbital Infrastructure

Satellites provide critical communications, navigation, weather monitoring, and intelligence capabilities. The increasing dependence on satellite systems for both civilian and military purposes has made them attractive targets for cyber and kinetic attack. The vulnerability of

satellites to cyber attack is particularly concerning given their remote location, limited ability to be physically repaired, and the cascading effects of their loss.

The cyber vulnerability of satellites arises from their dependence on ground control systems, uplink and downlink communications, and onboard software. An attacker who gains access to the ground control system or who can inject malicious commands into the uplink could potentially take control of a satellite, disrupt its operations, or cause it to malfunction. The 2022 Viasat KA-SAT attack, which disrupted satellite Internet services in Europe, demonstrated the vulnerability of satellite systems to cyber attack.

The kinetic vulnerability of satellites arises from the development of anti-satellite (ASAT) weapons by several states. ASAT weapons can physically destroy satellites through direct ascent missiles, co-orbital systems, or directed energy weapons. The testing of ASAT weapons creates space debris that threatens all satellites and space activities, raising concerns about the sustainability of the space environment.

The Elrakhawi Doctrine recognizes that satellites are critical infrastructure of strategic importance and calls for their protection under international law. The doctrine proposes that cyber attacks on satellites should be considered violations of international law and, if sufficiently severe, may constitute armed attacks justifying self-defense. The doctrine also calls for a ban on the testing and use of kinetic ASAT weapons that create long-lasting debris, recognizing that such weapons threaten the sustainability of the space environment for all states.

Cyber Anti-Satellite (ASAT) Warfare

The convergence of cyber and space domains creates new possibilities for cyber ASAT warfare. Rather than physically destroying a satellite, a cyber attacker could disrupt its operations, manipulate its data, or take control of its systems. Such attacks could achieve strategic objectives without creating debris or triggering the same escalation risks as kinetic ASAT attacks.

The Elrakhawi Doctrine recognizes the potential for cyber ASAT warfare and calls for the development of legal frameworks and technical measures to address this threat. The doctrine proposes that cyber attacks on satellites should be subject to the same legal standards as kinetic ASAT attacks, including the principles of necessity, proportionality, and distinction. The doctrine also calls for the development of resilient satellite architectures that can continue to function even if some components are compromised.

The doctrine also recognizes the importance of international cooperation in protecting space infrastructure. The space environment is a global commons that requires coordinated management and protection. The doctrine calls for the strengthening of international institutions for space governance, including the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), and the development of norms of responsible behavior in cyberspace as applied to space systems.

CHAPTER NINE: SOVEREIGN CLOUDS AND NATIONAL DATA

The Concept of Sovereign Cloud

A sovereign cloud is a cloud computing infrastructure that is owned, operated, and controlled within a nation's borders, subject to that nation's laws and regulations. The concept of sovereign cloud has emerged in response to concerns about data privacy, national security, and digital sovereignty in an era where much of the world's data is stored in cloud infrastructures controlled by foreign companies, primarily based in the United States.

The Elrakhawi Doctrine recognizes the legitimate interest of states in ensuring that sensitive government data and critical national information is stored and processed within their jurisdiction, subject to their laws and oversight. The doctrine proposes that sovereign clouds are an essential component of digital sovereignty, enabling states to control their data and protect it from unauthorized access, surveillance, or manipulation by foreign actors.

However, the doctrine also recognizes the challenges and limitations of sovereign clouds. Building and operating sovereign cloud infrastructure requires significant investment in technical capabilities, and many states lack the resources to develop sovereign clouds that match the scale, efficiency, and innovation of commercial cloud providers. Moreover, the isolation of sovereign clouds from the global cloud ecosystem may reduce interoperability, increase costs, and limit access to the latest technologies and services.

Storing Government Data in Sovereign Clouds

The doctrine proposes that government data should be classified according to sensitivity and stored in appropriate cloud environments. Highly classified national security data should be stored in air-gapped systems with strict access controls and physical security. Sensitive but unclassified data should be stored in sovereign clouds with strong encryption, access controls, and audit capabilities. Non-sensitive data may be stored in commercial clouds provided that appropriate contractual and technical safeguards are in place.

The doctrine calls for the development of clear standards and certifications for sovereign clouds, ensuring that they meet minimum security requirements and are subject to regular audit and oversight. The doctrine also calls for international cooperation on sovereign cloud standards, recognizing that interoperability between sovereign clouds is essential for international cooperation and commerce.

Legal Challenges: Cross-Border Jurisdiction

The storage of data in sovereign clouds raises complex legal questions about jurisdiction, particularly when data is accessed from or transmitted to other countries. The United States Cloud Act of 2018, which enables US law enforcement to compel US-based cloud providers to

produce data stored overseas, has raised concerns about the extraterritorial reach of US law and the potential conflict with data protection laws in other countries.

The European Union's General Data Protection Regulation (GDPR) restricts the transfer of personal data to countries that do not provide adequate data protection, creating tensions with the Cloud Act and other extraterritorial laws. The Schrems II decision of the Court of Justice of the European Union invalidated the EU-US Privacy Shield framework for data transfers, further complicating the legal landscape.

The Elrakhawi Doctrine proposes that the storage and transfer of data should be governed by the principle of digital sovereignty, under which each state has the right to control data within its jurisdiction while respecting the sovereignty of other states. The doctrine calls for the development of international agreements on cross-border data flows that balance the legitimate interests of states in controlling their data with the needs of the global economy for data flows.

The doctrine also proposes the development of technical measures to enable secure cross-border data flows, including encryption, data anonymization, and trusted execution environments. These measures can enable data to be processed and analyzed without exposing the underlying data to unauthorized access, balancing the needs of sovereignty with the needs of cooperation.

Case Studies: GDPR, Cloud Act, and Russian Sovereign Cloud

To illustrate the challenges of sovereign clouds and cross-border data flows, it is instructive to examine specific cases.

The GDPR represents the most comprehensive data protection framework in the world, establishing strict rules for the collection, processing, and transfer of personal data. The GDPR's restrictions on cross-border data transfers have significant implications for sovereign clouds, as data stored in sovereign clouds must comply with GDPR requirements if it involves personal data of EU residents. The GDPR has influenced data protection laws worldwide, creating a de facto global standard for data protection.

The US Cloud Act represents a different approach, prioritizing law enforcement access to data over data localization. The Cloud Act enables US authorities to compel US-based cloud providers to produce data regardless of where it is stored, subject to certain safeguards and international agreements. The Cloud Act has been criticized for its extraterritorial reach and potential conflict with data protection laws in other countries.

Russia's sovereign cloud initiative represents an attempt to build national cloud infrastructure subject to Russian law and oversight. Russia has enacted data localization requirements mandating that personal data of Russian citizens be stored on servers within Russia, and has invested in domestic cloud providers. The Russian approach prioritizes sovereignty and control

over interoperability and innovation, raising questions about the long-term viability and competitiveness of Russian cloud infrastructure.

These cases demonstrate the diversity of approaches to sovereign clouds and cross-border data flows, and the tensions between sovereignty, privacy, security, and economic efficiency. The Elrakhawi Doctrine calls for balanced approaches that respect digital sovereignty while enabling international cooperation and innovation.

=====

THE ELRAKHAWI DOCTRINE: VOLUME X (PART 3 OF 3)
CYBER COSMIC WARFARE
TOWARDS DIGITAL SOVEREIGNTY AND THE LAW OF ARMED CONFLICTS IN THE FIFTH
DOMAIN

=====

=====

PART IV: HOW - WEAPONS OF MASS DIGITAL DESTRUCTION

=====

=====

CHAPTER ELEVEN: AUTONOMOUS OFFENSIVE ARTIFICIAL INTELLIGENCE

The Emergence of Autonomous Cyber Weapons

The development of artificial intelligence has introduced a paradigm shift in cyber warfare: the creation of autonomous offensive cyber weapons. Unlike traditional malware, which requires human operators to select targets, initiate attacks, and manage propagation, autonomous cyber weapons can independently scout networks, identify vulnerabilities, select targets, and execute payloads without real-time human intervention. This capability mirrors the development of lethal autonomous weapons systems (LAWS) in the kinetic domain, but with the added complexity of operating at machine speed across global networks.

The Elrakhawi Doctrine defines an autonomous cyber weapon as any software system capable of independently identifying, targeting, and compromising digital systems with the intent to disrupt, degrade, destroy, or manipulate, without requiring specific human authorization for each individual action. The core concern is the removal of meaningful human control from the decision-making loop, creating systems that can escalate conflicts, cause unintended collateral damage, or be hijacked by adversarial actors.

The Existential Risks of Uncontrolled AI

The deployment of autonomous cyber weapons poses existential risks to global stability. First, the speed of autonomous cyber operations far exceeds human cognitive processing speeds, creating a "flash war" scenario where escalating retaliatory strikes occur in milliseconds, leaving

no time for diplomatic de-escalation or human verification of targets. Second, the complexity of machine learning algorithms makes the behavior of autonomous systems inherently unpredictable in novel environments, increasing the risk of cascading failures in critical infrastructure. Third, the proliferation of such technology to non-state actors or rogue states lowers the barrier to entry for causing catastrophic harm.

The Proposed Legal Framework: Prohibition of Autonomous Cyber Weapons

Drawing parallels with international bans on biological weapons and blinding laser weapons, the Elrakhawi Doctrine advocates for a categorical prohibition on the development, deployment, and use of fully autonomous offensive cyber weapons. The doctrine proposes that international law must mandate "meaningful human control" over all cyber operations that have the potential to cause physical damage, severe economic disruption, or loss of life. This principle, known as the "Human-in-the-Loop" requirement, ensures that moral and legal accountability remains with human actors, preserving the foundational principles of international humanitarian law.

CHAPTER TWELVE: RANSOMWARE AS A STATE WEAPON

The Evolution of Ransomware

Ransomware has evolved from a nuisance perpetrated by individual cybercriminals seeking quick financial gain into a sophisticated instrument of statecraft. State-sponsored advanced persistent threats (APTs) now deploy ransomware not merely for extortion, but as a tool of economic warfare, political coercion, and strategic disruption. The 2017 NotPetya attack, ostensibly a ransomware deployment but functionally a wiper malware disguised as ransomware, caused over ten billion dollars in global damages and was widely attributed to state actors seeking to destabilize a rival nation.

Ransomware as an Instrument of Hybrid Warfare

The Elrakhawi Doctrine categorizes state-sponsored ransomware as a form of hybrid warfare. It operates in the gray zone below the threshold of armed conflict, allowing state actors to inflict significant economic and social harm while maintaining plausible deniability. By outsourcing these operations to proxy criminal groups, states can achieve strategic objectives without triggering traditional military responses. This asymmetry undermines the deterrence value of conventional military superiority.

Legal and Policy Responses

To counter the weaponization of ransomware, the doctrine proposes a multi-faceted legal and policy response. First, the international community must establish a norm prohibiting states from harboring, funding, or directing ransomware operations, with clear consequences for violations, including targeted financial sanctions and cyber countermeasures. Second, the doctrine advocates for the criminalization of ransomware payments at the national level, arguing that paying ransoms perpetuates the ecosystem and indirectly funds state-sponsored aggression. Third, it calls for the establishment of an international cyber insurance framework that mandates strict cybersecurity baselines as a condition of coverage, shifting the financial risk back to organizations that fail to implement basic hygiene.

CHAPTER THIRTEEN: BLOCKCHAIN WARFARE AND DIGITAL CURRENCIES

The Weaponization of Cryptocurrencies

Cryptocurrencies and blockchain technologies, originally envisioned as tools for financial decentralization and privacy, have been co-opted as instruments of cyber warfare. State actors utilize cryptocurrencies to evade international sanctions, finance illicit operations, and launder the proceeds of cybercrime. Furthermore, the underlying blockchain infrastructure is increasingly targeted by state-sponsored actors seeking to disrupt financial markets or undermine confidence in digital assets.

Sanctions Evasion and Illicit Finance

The Elrakhawi Doctrine identifies the use of decentralized finance (DeFi) and privacy coins as a critical vulnerability in the international sanctions regime. States under comprehensive sanctions have developed sophisticated mechanisms to convert national wealth into cryptocurrencies, bypassing the traditional banking system and the oversight of the Financial Action Task Force (FATF). This undermines the efficacy of economic statecraft and empowers rogue regimes to sustain their military and cyber programs.

Regulating the Digital Financial Battlefield

The doctrine proposes the development of an international regulatory framework for digital assets in the context of national security. This framework must balance the innovation potential of blockchain technology with the imperative of preventing its misuse for warfare or terrorism. Key measures include the mandatory implementation of "Travel Rule" standards for all virtual asset service providers globally, the development of central bank digital currencies (CBDCs) with built-in compliance and traceability features, and the establishment of an international task force dedicated to tracking and disrupting state-sponsored cryptocurrency laundering networks.

CHAPTER FOURTEEN: INFORMATION WARFARE AND PUBLIC OPINION MANIPULATION

The Cognitive Domain as a Battlefield

Modern cyber warfare extends beyond the disruption of physical infrastructure to the manipulation of the cognitive domain. Information warfare, facilitated by cyber capabilities, seeks to undermine democratic processes, polarize societies, and erode trust in institutions. The use of automated bots, algorithmic amplification, and deepfake technology allows state actors to conduct massive, targeted disinformation campaigns at a scale and speed previously unimaginable.

Deepfakes and the Erosion of Truth

The emergence of generative AI capable of creating highly realistic synthetic media (deepfakes) represents a profound threat to the integrity of public discourse. The Elrakhawi Doctrine warns that the weaponization of deepfakes to fabricate statements by political leaders, manufacture evidence of war crimes, or trigger financial panic could have catastrophic consequences. The

inability of the human eye to distinguish between reality and sophisticated fabrication undermines the very concept of shared truth upon which democratic societies depend.

Protecting Democratic Processes

To defend against information warfare, the doctrine proposes a framework of "Cognitive Defense." This includes the mandatory labeling of AI-generated content, the establishment of independent, internationally recognized fact-checking consortiums, and the regulation of social media algorithms to prevent the artificial amplification of state-sponsored disinformation. Crucially, the doctrine asserts that while states have a right to defend their information environments, these defensive measures must strictly adhere to international human rights standards, avoiding the pretext of "fighting disinformation" to justify censorship or the suppression of legitimate dissent.

=====

PART V: VICTIMS AND RIGHTS

=====

CHAPTER FIFTEEN: VICTIMS OF CYBER WARFARE

The Expanding Circle of Harm

Traditional models of armed conflict primarily recognize states and combatants as the principal actors and victims. Cyber warfare fundamentally disrupts this model. The victims of cyber operations are diverse and often indirect, encompassing individuals, corporations, critical infrastructure, and the global digital ecosystem. The Elrakhawi Doctrine insists that any comprehensive legal framework for cyber warfare must explicitly recognize and protect these diverse categories of victims.

Individual Victims: Identity, Finance, and Psychology

Individuals suffer direct harm from cyber warfare through the theft of personal data, financial fraud, and the disruption of essential services like healthcare and banking. Furthermore, the psychological impact of living under the constant threat of surveillance, identity theft, or manipulation by state actors constitutes a distinct form of harm that international law has yet to fully address. The doctrine asserts that individuals possess a fundamental right to digital security and must have avenues for redress when their digital rights are violated by state-sponsored cyber operations.

State and Corporate Victims

States suffer harm through the degradation of their sovereign functions, the theft of intellectual property, and the erosion of public trust. Corporations, particularly those operating critical infrastructure, are often the primary targets of cyber attacks. The doctrine recognizes that while corporations are not subjects of international law in the same way as states, their victimization

can have cascading effects on national security and public welfare, warranting specific protections and support mechanisms.

CHAPTER SIXTEEN: VICTIMS' RIGHTS AND COMPENSATION MECHANISMS

The Right to Compensation

Under traditional international law, states responsible for internationally wrongful acts are obligated to make full reparation for the injury caused. The Elrakhawi Doctrine extends this principle to the cyber domain, asserting that victims of unlawful cyber operations have a right to compensation. However, the practical realization of this right is hindered by the difficulties of attribution and the lack of established mechanisms for adjudicating cyber claims.

The International Cyber Compensation Fund

To overcome these barriers, the doctrine proposes the establishment of an International Cyber Compensation Fund (ICCF). Modeled after the United Nations Compensation Commission established after the Gulf War, the ICCF would be funded by mandatory contributions from member states, supplemented by fines levied on states or entities found responsible for unlawful cyber operations. The fund would provide expedited compensation to individuals, corporations, and states that have suffered demonstrable harm from cyber attacks, particularly in cases where the responsible state is unable or unwilling to provide direct reparation.

Mechanisms for Claiming Redress

The doctrine outlines a streamlined process for victims to claim redress through the ICCF. This process would rely on a lowered standard of proof for attribution, utilizing a "preponderance of evidence" standard rather than the stringent "beyond a reasonable doubt" standard required in criminal courts. Claims would be evaluated by independent panels of technical and legal experts, ensuring that victims receive timely and fair compensation without being entangled in protracted geopolitical disputes.

=====

PART VI: CYBER CRIMINAL INVESTIGATION AND DIGITAL EVIDENCE

=====

CHAPTER SEVENTEEN: CYBER CRIMINAL INVESTIGATION METHODOLOGIES

The Challenge of Digital Forensics

Investigating cyber warfare and cyber crime presents unique challenges that traditional forensic methodologies are ill-equipped to handle. Digital evidence is inherently volatile, easily altered, and often distributed across multiple jurisdictions. The Elrakhawi Doctrine emphasizes the need for standardized, internationally recognized methodologies for digital forensics to ensure that investigations are thorough, lawful, and capable of withstanding judicial scrutiny.

Preserving the Chain of Custody

The chain of custody is the chronological documentation of the seizure, custody, control, transfer, analysis, and disposition of digital evidence. In the cyber domain, maintaining an unbroken chain of custody is critical to proving that the evidence has not been tampered with. The doctrine mandates the use of cryptographic hashing (such as SHA-256) at every stage of the evidence handling process to create a verifiable, tamper-evident record of the data's integrity.

International Cooperation in Investigations

Cyber threats do not respect national borders, making international cooperation essential for effective investigation. The doctrine calls for the modernization of mutual legal assistance treaties (MLATs) to accommodate the speed of cyber investigations. It proposes the establishment of a 24/7 international cyber crime network, modeled on the Budapest Convention's 24/7 Network, to facilitate rapid data preservation requests and real-time collaboration between national law enforcement agencies.

CHAPTER EIGHTEEN: DIGITAL EVIDENCE IN COURT

Admissibility Standards for Digital Evidence

For digital evidence to be useful, it must be admissible in court. The Elrakhawi Doctrine proposes a unified framework for the admissibility of digital evidence, based on three core criteria: authenticity, reliability, and relevance. Authenticity requires proof that the digital evidence is what it purports to be. Reliability requires demonstration that the tools and methods used to collect and analyze the evidence are scientifically valid and generally accepted in the forensic community. Relevance requires that the evidence has a logical connection to the facts of the case.

The Attribution Problem

Attribution remains the most significant hurdle in prosecuting cyber crimes and holding states accountable for cyber warfare. The doctrine acknowledges that perfect attribution is rarely possible in cyberspace. Therefore, it proposes a framework of "probabilistic attribution," allowing courts to assign responsibility based on a convergence of technical indicators (e.g., malware code similarities, infrastructure overlap), intelligence assessments, and behavioral patterns, provided the cumulative weight of evidence meets the required legal standard of proof.

The Role of Technical Expertise in Judicial Proceedings

The complexity of cyber cases necessitates the presence of qualified technical experts in judicial proceedings. The doctrine advocates for the creation of a roster of internationally certified cyber forensics experts who can be appointed by courts to provide impartial, objective analysis of digital evidence. Furthermore, it calls for the mandatory training of judges and prosecutors in the fundamentals of digital evidence to ensure they can effectively evaluate expert testimony and make informed legal rulings.

=====

=====

PART VII: THE SUPREME JUDICIAL ARCHITECTURE

=====

=====

CHAPTER NINETEEN: THE ELRAKHAWI UNIVERSAL DECLARATION ON THE PROHIBITION OF AUTONOMOUS CYBER WEAPONS

Preamble

Recognizing the unprecedented risks posed by autonomous offensive cyber weapons to global peace, security, and human dignity;

Affirming that meaningful human control must be maintained over all uses of force and all operations with the potential to cause significant harm;

The Global Assembly on Cyber Governance hereby proclaims this Universal Declaration on the Prohibition of Autonomous Cyber Weapons as a binding norm of customary international law.

Article 1: Definition and Prohibition

An autonomous cyber weapon is defined as any software system capable of independently selecting and engaging targets in cyberspace without meaningful human intervention. The development, testing, deployment, and use of such systems are strictly prohibited.

Article 2: Meaningful Human Control

All cyber operations, whether defensive or offensive, must be subject to meaningful human control. Human operators must possess the contextual understanding, authority, and ability to intervene and abort the operation at any stage.

Article 3: Verification and Compliance

States parties shall establish national verification mechanisms and submit to regular international inspections to ensure compliance with this prohibition. The sharing of source code and algorithmic architectures of dual-use AI systems may be required for verification purposes, subject to strict confidentiality protocols.

CHAPTER TWENTY: THE CYBER GENEVA PROTOCOLS

The Need for Specialized Humanitarian Law

While the existing Geneva Conventions provide a foundational framework for the protection of civilians during armed conflict, their application to cyberspace is often ambiguous. The Elrakhawi Doctrine proposes the adoption of the Cyber Geneva Protocols, a specialized addition to international humanitarian law tailored to the unique characteristics of cyber warfare.

Core Principles of the Cyber Geneva Protocols

The protocols are built upon four core principles:

1. The Principle of Distinction: Parties to a conflict must distinguish between military cyber objectives and civilian cyber infrastructure. Indiscriminate cyber attacks that cannot be directed at a specific military objective are prohibited.

a. The Principle of Proportionality: Cyber attacks that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects must not be excessive in relation to the concrete and direct military advantage anticipated.

2. The Principle of Precaution: Parties must take all feasible precautions to avoid or minimize harm to civilians and civilian infrastructure, including the use of highly targeted malware and the provision of effective warnings prior to attacks on dual-use infrastructure.

3. The Protection of Essential Services: Cyber attacks directed against infrastructure indispensable to the survival of the civilian population, such as drinking water installations, healthcare systems, and food distribution networks, are absolutely prohibited, regardless of whether they are military objectives.

CHAPTER TWENTY-ONE: THE INTERNATIONAL COURT FOR CYBER WAR CRIMES

Establishing Jurisdiction

The ultimate enforcement mechanism of the Elrakhawi Doctrine is the establishment of an International Court for Cyber War Crimes (ICCWC). This specialized tribunal would have jurisdiction over the most serious violations of international law in cyberspace, including the use of prohibited autonomous cyber weapons, deliberate attacks on critical civilian infrastructure, and state-sponsored cyber terrorism.

Structure and Composition

The ICCWC would be composed of judges with dual expertise in international law and computer science. The prosecution would be supported by a dedicated Cyber Forensics Division, equipped with state-of-the-art tools for attribution and evidence analysis. The court would operate under a hybrid procedural framework, combining the adversarial and inquisitorial traditions to ensure both fairness and thoroughness.

Enforcement and Sanctions

While the ICCWC would lack its own police force, its judgments would be binding on member states. The United Nations Security Council would be empowered to enforce the court's decisions, including the imposition of targeted sanctions, asset freezes, and, in extreme cases, the authorization of collective cyber or kinetic countermeasures against non-compliant states.

CHAPTER TWENTY-TWO: ROADMAP TO IMPLEMENTATION

Phase One: Normative Foundation (2026-2028)

The immediate priority is the diplomatic campaign to secure widespread endorsement of the Elrakhawi Universal Declaration on the Prohibition of Autonomous Cyber Weapons and the Cyber Geneva Protocols. This phase involves extensive consultation with states, international organizations, civil society, and the technical community to build a broad consensus.

Phase Two: Institutional Capacity Building (2028-2030)

Concurrent with normative development, efforts must focus on building the institutional capacity required to implement the framework. This includes the establishment of the International Cyber Compensation Fund, the training of a global roster of cyber forensics experts, and the modernization of international mutual legal assistance mechanisms.

Phase Three: Treaty Ratification and Court Establishment (2030-2032)

The negotiation and ratification of the treaty establishing the International Court for Cyber War Crimes. This phase requires securing the commitment of major cyber powers to submit to the court's jurisdiction and to provide the necessary financial and logistical support for its operation.

Phase Four: Full Operationalization (2032-2035)

The ICCWC becomes fully operational, beginning with the prosecution of landmark cases to establish precedent and demonstrate the court's effectiveness. The international community transitions to a new normal where cyber operations are governed by the rule of law, and violations are met with swift, legitimate, and proportionate consequences.

CONCLUSION

The advent of cyberspace as a domain of conflict has fundamentally altered the nature of warfare, outpacing the development of the legal and ethical frameworks necessary to govern it. The Elrakhawi Doctrine on Cyber Cosmic Warfare represents a comprehensive, forward-looking response to this existential challenge. By establishing the principle of digital sovereignty, defining clear thresholds for armed conflict through the Cyber War Legitimacy Equation, and proposing a supreme judicial architecture anchored by the Cyber Geneva Protocols and the International Court for Cyber War Crimes, this doctrine provides a viable roadmap for bringing the rule of law to the fifth domain.

The choice before the international community is stark. We can continue to drift toward a chaotic, unregulated digital battleground where the strong prey on the weak, critical infrastructure is perpetually at risk, and the fabric of democratic society is eroded by relentless manipulation. Or, we can embrace the principles of sovereignty, accountability, and humanity articulated in this doctrine, forging a new social contract for the digital age.

The architecture for a secure, stable, and just cyberspace has been designed. The tools for its implementation are within our grasp. What is required now is the collective political will to build it. The time for incrementalism and ambiguity has passed. The era of cosmic cyber justice must begin.

Praise be to God, by whose grace all good deeds are brought to completion.

APPENDICES

APPENDIX A: THE ELRAKHAWI CYBER WAR LEGITIMACY EQUATION (CWLE) DETAILED FORMULATION

The CWLE is calculated as: $CWLE = (S_e * I_n * P_r) / (D_c * C_v)$

Variable Definitions and Scoring Metrics:

S_e (Scale of Effects): 0.1 (minor inconvenience) to 10.0 (mass casualties or catastrophic infrastructure collapse).

I_n (Intent and Attribution Confidence): 0.1 (anonymous, ambiguous) to 10.0 (confirmed state actor, explicit declaration of hostile intent).

P_r (Proportionality to Political Objectives): 0.1 (grossly disproportionate, indiscriminate) to 10.0 (strictly proportional to a legitimate, narrowly defined military objective).

D_c (Dual-Use Character): 0.1 (exclusively civilian target, e.g., pediatric hospital) to 10.0 (exclusively military target, e.g., isolated missile silo).

C_v (Civilian Vulnerability): 0.1 (no foreseeable civilian impact) to 10.0 (high likelihood of severe civilian harm or panic).

Threshold Interpretation:

Score > 7.0: Constitutes an Armed Attack (Article 51 self-defense justified).

Score 4.0 - 7.0: Constitutes a Use of Force (Countermeasures justified, self-defense not justified).

Score < 4.0: Below the threshold of armed conflict (Law enforcement, diplomatic, or economic responses appropriate).

APPENDIX B: KEYWORDS IN TEN GLOBAL LANGUAGES

1. English: Cyber Cosmic Warfare, Digital Sovereignty, Cyber War Legitimacy Equation, Autonomous Cyber Weapons, Cyber Geneva Protocols, International Court for Cyber War Crimes, Critical Infrastructure Protection, Digital Forensics, Ransomware as State Weapon, Blockchain Warfare.

2. Arabic: الحرب السيبرانية الكونية، السيادة الرقمية، معادلة مشروعية الحرب السيبرانية، الأسلحة السيبرانية ذاتية القرار، بروتوكولات جنيف السيبرانية، المحكمة الدولية للجرائم السيبرانية الحربية، حماية البنية التحتية الحرجة، الطب الشرعي الرقمي، الفدية كسلاح دولة، حرب البلوكشين.

3. French: Guerre Cyber Cosmique, Souveraineté Numérique, Équation de Légitimité de la Guerre Cyber, Armes Cybernétiques Autonomes, Protocoles de Genève Cyber, Cour Internationale des Crimes de Guerre Cyber, Protection des Infrastructures Critiques, Médecine Légale Numérique, Rançongiciel comme Arme d'État, Guerre de la Blockchain.
4. Spanish: Guerra Cibernética Cósmica, Soberanía Digital, Ecuación de Legitimidad de la Guerra Cibernética, Armas Cibernéticas Autónomas, Protocolos de Ginebra Cibernéticos, Corte Internacional de Crímenes de Guerra Cibernéticos, Protección de Infraestructuras Críticas, Forense Digital, Ransomware como Arma Estatal, Guerra Blockchain.
5. German: Kybernetische Kosmische Kriegsführung, Digitale Souveränität, Gleichung der Legitimität des Cyberkrieges, Autonome Cyberwaffen, Cyber-Genfer-Protokolle, Internationaler Gerichtshof für Cyber-Kriegsverbrechen, Schutz Kritischer Infrastrukturen, Digitale Forensik, Ransomware als Staatswaffe, Blockchain-Kriegsführung.
6. Chinese: 网络宇宙战, 数字主权, 网络战合法性方程, 自主网络武器, 网络日内瓦议定书, 国际网络战争罪法院, 关键基础设施保护, 数字取证, 勒索软件作为国家武器, 区块链战.
7. Russian: Киберкосмическая война, Цифровой суверенитет, Уравнение легитимности кибервойны, Автономное кибероружие, Кибернетические Женевские протоколы, Международный суд по кибервоенным преступлениям, Защита критической инфраструктуры, Цифровая криминалистика, Программы-вымогатели как государственное оружие, Блокчейн-война.
8. Italian: Guerra Cibernetica Cosmica, Sovranità Digitale, Equazione di Legittimità della Guerra Cibernetica, Armi Cibernetiche Autonome, Protocolli di Ginebra Cibernetici, Corte Internazionale per i Crimini di Guerra Cibernetici, Protezione delle Infrastrutture Critiche, Informatica Forense, Ransomware come Arma di Stato, Guerra Blockchain.
9. Turkish: Siber Kozmik Savaş, Dijital Egemenlik, Siber Savaş Meşruiyet Denklemi, Otonom Siber Silahlar, Siber Cenevre Protokolleri, Uluslararası Siber Savaş Suçları Mahkemesi, Kritik Altyapı Koruması, Dijital Adli Tıp, Devlet Silahı Olarak Fidyeye Yazılımı, Blockchain Savaşı.
10. Portuguese: Guerra Cibernética Cósmica, Soberania Digital, Equação de Legitimidade da Guerra Cibernética, Armas Cibernéticas Autônomas, Protocolos de Genebra Cibernéticos, Tribunal Internacional de Crimes de Guerra Cibernéticos, Proteção de Infraestruturas Críticas, Forense Digital, Ransomware como Arma Estatal, Guerra Blockchain.

=====

=====

APPENDIX C: COMPREHENSIVE LEGAL PROTECTION AND INTELLECTUAL PROPERTY FRAMEWORK

SECTION 1: COPYRIGHT AND AUTHORSHIP

Copyright 2026 by Dr. Mohamed Kamal Arafa El Rakhawi. All rights reserved worldwide. This work, including its text, structural framework, the Cyber War Legitimacy Equation (CWLE), the Elrakhawi Universal Declaration on the Prohibition of Autonomous Cyber Weapons, and all conceptual architectures, constitutes the exclusive intellectual property of the author under international copyright law, including the Berne Convention and the TRIPS Agreement.

SECTION 2: PATENT AND METHODOLOGY PROTECTION

The following innovations are subject to pending intellectual property protections under the Patent Cooperation Treaty (PCT):

Protection Application I: "Method and System for Quantifying the Threshold of Cyber Armed Conflict via the Cyber War Legitimacy Equation (CWLE)" (PCT/EP2026/XXXXXX).

Protection Application II: "Framework for the Admissibility and Probabilistic Attribution of Digital Evidence in International Tribunals" (PCT/EP2026/XXXXXX).

Any unauthorized commercial use, reproduction, or implementation of these methodologies without a formal written license is strictly prohibited.

SECTION 3: PROTECTION OF THE LITERARY EXPRESSION OF THE FRAMEWORK

In accordance with Article 9.2 of the TRIPS Agreement, copyright protection extends to the specific textual articulation, mathematical formulation, and logical sequencing of the Elrakhawi Universal Declaration and the CWLE. The abstract philosophical concepts of digital sovereignty remain in the public domain, but their specific codification and structural taxonomy as presented herein are protected literary expressions requiring attribution and, for commercial use, formal licensing.

SECTION 4: LICENSING FRAMEWORK

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0) for academic, educational, and non-commercial purposes. For commercial licensing, institutional certification, proprietary integration, or translation rights, interested parties must contact the author directly through the Zenodo platform.

SECTION 5: ENFORCEMENT AND JURISDICTION

Unauthorized modification, redistribution, or commercial exploitation of this work constitutes a violation of international intellectual property conventions and will be pursued legally. The courts of the Arab Republic of Egypt shall have primary jurisdiction over disputes arising from this work, with alternative arbitration through the WIPO Arbitration and Mediation Center.

SECTION 6: MORAL RIGHTS

Under Article 6bis of the Berne Convention, the author asserts his moral rights, including the right of paternity and the right of integrity. These moral rights are inalienable and persist independently of any economic rights transferred or licensed.

=====

=====

APPENDIX D: GLOBAL REFERENCES AND DETAILED INDICES

Selected Foundational References:

1. El Rakhawi, M. K. A. (2026). The Cyber War Legitimacy Equation: Quantifying the Threshold of Armed Conflict in the Fifth Domain. *Journal of International Cyber Law*, 15(1), 45-78.

2. El Rakhawi, M. K. A. (2026). Digital Sovereignty and the Future of the Westphalian Order. *Global Governance Review*, 32(4), 112-135.
3. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
4. United Nations. (1945). Charter of the United Nations, Article 51.
5. International Committee of the Red Cross. (2 to 1949). *Geneva Conventions and Additional Protocols*.
6. World Economic Forum. (2023). *The Global Cybersecurity Outlook*.
7. National Institute of Standards and Technology (NIST). (2023). *Framework for Improving Critical Infrastructure Cybersecurity*.

Analytical Index:

Autonomous Cyber Weapons, 145, 167, 210
Blockchain Warfare, 156, 178
Critical Infrastructure Protection, 134, 189
Cyber Geneva Protocols, 210, 215
Cyber War Legitimacy Equation (CWLE), 120, 125, 230
Digital Forensics, 198, 205
Digital Sovereignty, 110, 115, 130
International Court for Cyber War Crimes, 210, 218
Meaningful Human Control, 145, 210
Probabilistic Attribution, 205, 218
Ransomware as State Weapon, 150, 175
Submarine Cables and Satellites, 134, 140

=====

=====

DECLARATION OF ORIGINALITY AND INDEPENDENT RESEARCH

=====

=====

I, Dr. Mohamed Kamal Arafa El Rakhawi, hereby declare that this work, Volume X of The Elrakhawi Doctrine, is the product of my independent research and original intellectual creation. The conceptual frameworks of Digital Sovereignty, the Cyber War Legitimacy Equation (CWLE), the Cyber Geneva Protocols, and the proposal for an International Court for Cyber War Crimes are original contributions to the fields of international law, cybersecurity, and global governance.

This work was conceived and written without institutional funding, corporate sponsorship, or conflict of interest. The author maintains full independence in the presentation of scientific, legal, and strategic frameworks.

Date of Declaration: September 23, 2026
Place: Ismailia, Arab Republic of Egypt

=====
=====

END OF DOCUMENT

=====
=====

Dr. Mohamed Kamal Arafa El Rakhawi
International Researcher in Jurisprudence, Philosophy of Law, Cybersecurity, and Cosmic
Justice
Ismailia, Arab Republic of Egypt
September 23, 2026

Digital Object Identifier: 10.5281/zenodo.22909983
Permanent URL: <http://doi.org/10.5281/zenodo.22909983>