CyberIR@MIT
Knowledge for Science, Policy, Practice

Nazli Choucri
Professor
Political Science Department
Massachusetts Institute of Technology

Lauren Fairman
Research Affiliate
Political Science Department
Massachusetts Institute of Technology

Gaurav Agarwal
Alumnus
Sloan School of Management
Massachusetts Institute of Technology

October 5, 2021, Revised July 9, 2022

Abstract

This paper presents a brief introduction to *CyberIR@MIT*—a dynamic, interactive knowledge and networking system focused on the evolving, diverse, and complex interconnections of cyberspace and international relations. The goal is to highlight key theoretical, substantive, empirical and networking issues.

CyberIR@MIT is anchored in a multidimensional ontology. It was initially framed as an experiment during the MIT-Harvard collaboration on Explorations in Cyber International Relations (MIT, 2009–2014) to serve as a forum for quality-controlled content and materials generated throughout the research project.

The vision for *CyberIR@MIT* is shaped by the research for Cyberpolitics in International Relations, a book written by Nazli Choucri and published by MIT Press in 2012. The operational approach to the knowledge system is influenced by the Global System for Sustainable Development (GSSD), developed earlier and focused on challenges of system sustainability. *CyberIR@MIT* gradually evolved into a knowledge-based system of human interactions in cyberspace and international relations, all embedded in the overarching natural system.

The method consists of differentiating among the various facets of human activity in (i) cyberspace, (ii) international relations, and (iii) the intersection of the cyber and "real." It includes problems created by humans and solution strategies, as well as enabling functions and capabilities, on the one hand, and impediments to behavior and associated barriers, on the other. See https://cyberir.mit.edu for functions. The value of this initiative lies in its conceptual foundations and method of knowledge representation—embedded in an interactive system for knowledge submission, with search and retrieval functions.

Keywords:

Cyber-International Relations, Knowledge Management; Cyberspace & International Relations Intersections; Governance & Institutions; Conflict & War; Cybersecurity & Sustainability; System State; System Problem; Scientific & Technological Solutions & Strategies; Socio-Economic & Political Solutions & Strategies.

Funding:

Supported by Department of Political Science Department at Massachusetts Institute of Technology and the Minerva Program of US Department of Defense.

Website

Visit https://cyberir.mit.edu for submission of materials.

Table of Contents

List of Figures

1 What is *CyberIR@MIT*?

> ***CyberIR@MIT is a dynamic, interactive ontology-based knowledge system focused on the evolving, diverse & complex interconnections of cyberspace & international relations.***

Almost everyone recognizes that cyberspace is a fact of daily life. Given its ubiquity, scale, and scope, cyberspace—including the Internet, the billions of computers it connects, its management, and the experience it enables—has become a central feature of the world we live in and has created a fundamentally new reality for almost everyone, everywhere.

At the same time, information and communication systems—the foundations of all human societies and social interactions—are accorded rather limited attention in all major theories of international relations. Despite the centrality of all forms of information exchange—in all contexts, cultures, conditions, or situations—the content of communications, conduits, and forms of connectivity remain more marginal than is appropriate in world politics or international relations more broadly defined.

Until recently, cyberspace was considered largely a matter of low politics, a term used to denote background conditions and routine decisions and processes. By contrast, high politics concern national security, core institutions, and decision systems that are critical to the state, its interests, and underlying values.

If the cumulative effects of normal activity shift the established dynamics of interaction, then the seemingly routine becomes increasingly politicized. Cyberspace is now a matter of high politics. We see many incidents of power and politics, conflict and competition, violence and war—all central features of world politics—increasingly manifested via cyber venues.

In addition, the fundamental differences between the characteristics of cyberspace (with the Internet at its core) and the traditional features of international relations often make it difficult to track changes in each domain individually, and almost impossible to do so at their intersection.

1.1 System Features

CyberIR@MIT spans technical, operational, socio-economic, and political issues, as well as decision and policy areas. System features consist of:

1. *Strategies* for integrating and organizing knowledge domains consisting of multi-dimensional, multi-sector, and multi-disciplinary content.
2. *Conceptual framework*, based on collaborative research regarding computer science and international relations in political science.

3. *Content representation*, anchored in an ontology based on multidisciplinary research and the knowledge base.
4. *Diverse functions* for the detailed display of knowledge content regarding individual or aggregated topics.
5. *Processes* to organize knowledge content with interrelated concepts in a nested, internally consistent form.
6. *Alternative search* and retrieval functions.
7. *Submission* process to capture knowledge-content in an internally consistent form.
8. *Evolving* knowledge content and repository base for emergent research.

1.2 Challenge

The question mark in Figure 1 below captures the challenge, namely, to reduce the gap in our understanding. This gap is augmented by differential rates of changes along the trajectory of each arrow. The dynamics embedded therein are driven by technology, policy, and practice. The challenge embedded in the question mark must be “unbundled” and its elements identified.

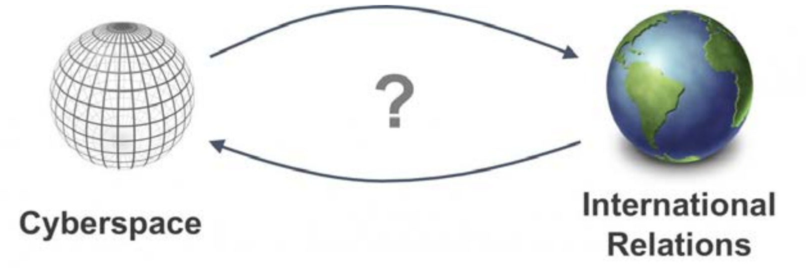


Figure 1. *Cyber-IR* system.

Source: Choucri and Clark (2019, p.5).

The challenge is to track the relationship between cyberspace and the conventional venues of international relations, reduce the disconnects, and help create the fundamental principles for aligning contemporary international relations theory, policy, and practice with the emergent complexities of the twenty-first century. Clearly, each of these two “spaces”—the cyber and the international—are defined by different core principles and characterized by distinct features of structure and process that enable, and are enabled by, a wide range of actors and activities.

The complexity of interconnections between *cyberspace* and *international relations* requires a multidisciplinary approach for assisting stakeholders—including governmental, scientific, and industrial stakeholders—in (a) sharing a common understanding of the challenges,

(b) accessing relevant knowledge bases, (c) exchanging expertise and perspectives, and (d) enhancing and improving all cyber-related capabilities.

CyberIR@MIT was designed in response to such daunting challenges. It is constructed around interactive knowledge resources and supported by a set of functionalities associated with research, policy, and practice. As an interactive knowledge system, it supports an evolving, quality-controlled database that includes submissions by users and provides search options over the entire knowledge base's component-domains (or topics), consisting of detailed knowledge-profiles of actors, actions, problems, and solution strategies.

1.3 Mission

The mission of *CyberIR@MIT* is to reduce barriers to our understanding of how cyberspace affects international relations and how international relations affect cyberspace. The objectives are three-fold:

1. *Conceptual & Scientific:*
    a. Develop a quality-controlled knowledge base
    b. Capture diverse methods, perspectives, and approaches
    c. Facilitate access to cutting-edge research
2. *Participation & Communication:*
    a. Support integrated perspectives on “virtual” and “real” dynamics
    b. Enable distribution of knowledge contributions
    c. Enhance knowledge-sharing with diverse options for search & retrieval
3. *Policy & Decision:*
    a. Enhance analytical and computational methods for decision-making
    b. Explore policy alternatives for security & “virtual” and “real” international stability
    c. Identify trade-offs, choices, and opportunity costs.

2 Explorations & Foundations for *CyberIR@MIT*

The explorations that shaped *CyberIR@MIT* were undertaken during the joint MIT- Harvard Research Project, *Explorations in Cyber International Relations* (http://ecir.mit.edu). Initially framed as an experiment to pull together the results of very diverse research interests (Choucri, 2016) the overall vision of the project was developed in the course of addressing and attempting to answer two broad questions, centered respectively in the theory and practice of international relations and in the technology and utilization of cyberspace. The result was the development of the framework for an integrated, joint Cyber-IR system.

For international relations, the highest-order question is how these issues matter and whether they have risen, or will rise, to the level of “high politics.” For cyberspace, with the Internet as its current core, the question is how its specific character shapes the nature of contention, which actors are empowered or not by its structure, and how to reason about it as a built artifact. The computational model for *CyberIR@MIT* is similar to that of the *Global System for Sustainable Development* (GSSD). See Choucri et al. (2007), and http://gssd.mit.edu, the evolving knowledge networking system:

1. With user-supporting functionalities,
2. Dedicated to sustainable development, and
3. Differentiates knowledge content between domains and dimensions.

Earlier modes of knowledge exploration provided ways of thinking about the issues—tools of reasoning, models of analysis, and the like—and did so in a global, geopolitical context. GSSD was designed to help identify and extend innovative approaches to sustainability—including enabling technologies, policies, and strategies. It tracks diverse aspects of the challenges, problems, and emergent solutions to date.

The ubiquity of the cyber arena and its pervasiveness in all forms of human activity calls for a meta-analysis, or an overarching investigation of the contours and interconnections of cyberspace and international relations (and international cyber- relations). Such analysis focuses on the co-evolution of these diverse domains and helps to identify the linkages between the international system (and international relations), on the one hand, and technological change (and cyberspace), on the other—through analytical, empirical, and observable terms.

2.1 Foundations

The reference to *co-evolution* involves matters of growth, development, security, stability, profit, control, governance, crime, and a wide range of related issues surrounding connectivity, conduits, and content, as well as emergent views of alternative futures. All elements are as central to international relations as they are to cyberspace.

2.1.1 Meta-Analysis

If the reality of cyberspace is changing the character of international relations, so the concerns of various states are changing the character of cyberspace. It is already apparent that political pressures impinge upon the current Internet in various parts of the world in order to render its architecture "in line" with power and politics. Recognizing this reality, initial explorations sought to sensitize computer scientists to the inherent but sometimes hidden influence of power and politics that bear on new architectures, new constructions of the Internet, and new frontiers of cyberspace. These also serves to improve the awareness of computer scientists of the potential for influence and leverage enabled, or even created by, the architecture of the Internet and all the attendant and operational features that sustain the core of cyberspace.

To some extent, there is a general tendency among analysts of international relations to make simplified assumptions about the character of cyberspace by pushing toward similarity with the known "real" domain that, in and of itself, may be problematic. To the extent that the state decides it must shape the character of cyberspace— irrespective of the wisdom of so proceeding— there are few guideposts or theories as to how to proceed in order to achieve this objective.

2.1.2 The Old & The New

Early in the twenty-first century, it was already apparent that the cyber domain would shape new parameters of international relations and new dimensions of international politics. Among the most salient features is the previously-noted creation of new actors— some with formal identities and others without—and their cyber empowerment, which is altering the traditional international decision landscape in potentially significant ways.

Concurrently, we see the growing use of cyber venues by nonstate groups whose objectives are to undermine the state or to alter its foundations.

In addition, growth in the number of cyber-centered actors increases the density of decision entities—each with new interests and new capabilities to pursue their interests—and thus increases the potential for intersections in spheres of influence, with possibilities for new and different types of contentions and conflicts.

With the benefit of hindsight, it is often noted how seemingly transparent and relatively "simple" was the world of the nineteenth century into the twentieth century. Gradually, it became more "complicated" as the victors' design for the postwar period required major innovations in the management of international activities. In retrospect, once more, what we had then understood as "complicated" is now more accurately described as "complex." With increasing cross-border interactions, entanglements that were viewed as “interdependence” in the twentieth century took on dynamics of their own, shaping what we refer to as "globalization."

As cyberspace shifted into the realm of “high politics,” it altered the international policy ecology, topography, and demography in profound ways. Interactions in cyberspace have shifted the balance of power among different actors, including the traditional state powers, and enabled weaker actors to influence or even threaten stronger actors (such as press reports of anonymous penetration incidences of U.S. government computer systems). This sort of shift has little precedence in world politics. We might view this situation—the players and their capabilities—as emergent symmetry.

2.1.3 Co-Evolution Dilemma

However framed, we are witnessing a potentially powerful shift in the nature of the “realities” around us. The increased influence of nonstate entities may well undermine the sanctity of sovereignty as the defining principle for the international system. The forgoing calls into question the effectiveness of traditional policy tools and responses crafted to deal with state-to-state interactions in a geopolitical world—with known threat actors and an arsenal of expected diplomatic or military responses.

All of this creates an added and inescapable problem for the state, the state system, and international relations, that is, the emergence of unprecedented threats to security. These threats carry a new label (cyber threats) to signal new vulnerabilities (cybersecurity) and—most vexing of all—can emanate from unknown sources (attribution problem). Invariably, these trends further reinforce the politicization of cyberspace and its salience in emergent policy discourses.

The basic, underlying premise is that the two domains are evolving into a system of interlocking and mutual influence that continues to shape each of these arenas while creating added, joint effects on society, the economy, politics, and all aspects of the human experience. The dilemma is rooted in the fact that the two systems are changing at different rates, and elements of each are also changing at different rates, thereby creating realities and uncertainties that are particularly difficult to anticipate or manage—let alone regulate. If cyberspace and international relations evolve as a joint system, then their differences must be addressed. Already, we appreciate that they are “held together” by very different concepts and practices of organization and order.

2.1.4 Daunting Questions

The co-evolution dilemma raises some daunting questions, for example: why is it, and how is it, that the sovereign state—which supported the construction of cyberspace with a vision of openness and freedom—is also engaged in various “denial of service” practices? How do different countries attempt to control data and information flows and monitor content or server connections? How is it (and why is it) that the “illegitimate” or damaging uses of the Internet are growing much faster than our ability to identify, control, or prevent them? Why is it that the power of the state—with its monopoly over the use of force, in theory—seems inadequate for responding to threats from the cyber domain?

The above refers to the co-evolution dilemma. It invariably touches upon and may even become dominated by the activities of nonstate actors and their management of the Internet so far. Overall, states recognize the dominance of the private sector in shaping the Internet, but few states are ready to accept or accommodate this reality. All are confronted with uncertainties regarding control of the cyber domain: *how*, *when*, and *why*? *Who* controls, and *where* are the control points?

2.1.5 Order & Authority

In social science parlance, what keeps a system together is a form of order supported by authority. Authority involves a claim of trust in social relationships in order to induce conformity and support for governing principles. So too, there is a special relationship between authority or source and subject, a relationship that is located in a particular, definable domain. This relationship is based on some form of consensus and is supported by prevailing norms, rules, and practices. This directionality—on matters of substance as well as context—forges a set of obligations. All of this is social order.

The international system is a system of states. The state can rely on the obedience of its citizens by establishing legal codes and punishing those who transgress. This, in conjunction with the inability of individuals to protect themselves from each other, forges the special relationship between the state and individuals. Generally, public authority dominates and social recognition of authority is expressed publicly.

The cyber domain—the entire arena anchored in the Internet—was constructed by private sector actors (albeit with support and funding from the dominant states). So far, authority over the operation of the Internet is based on performance and capability. More specifically, authority in the cyber domain is derived from innovation of the system we call the Internet and the operational capacity demonstrated by effective control of essential activities.

In this context, the role of private authority is self-generated by the construction of the new domain. These entities pursue their own interests, not necessarily those of the state or those of the market. They are strong enough to establish the rules of interaction over an issue-area and even to control the agenda for policy deliberation. Today, private authority is strong and salient in many parts of the world and for many issues of interest.

2.1.6 Conflict & War

Modes of conflict and of cooperation are well recognized in the "real" domain of international relations, as are matters of their scale and scope. The "virtual" arena also harbors various forms of conflict and cooperation. The former has led to a completely new vocabulary to represent various manifestations, such as “cyber threat,” “cybersecurity,” “cyber warfare,” or “cyber arms race”—to note the most obvious.

Given that the “new normal” in world politics of the cyber age is one that transcends state actors and actions, the conduct of conflict, violence, and warfare in the cyber domain is significantly different from tradition in international relations. A wide range of nonstate entities—known and unknown—operate in a highly dynamic and volatile international context.

The conduct of war in the “real” domain is inevitably adapting to, or changed by, the features of the “virtual” arena. The challenge is to recognize various modalities and the ways in which different actors seek to exert influence and shape the environment to support their goals.

2.1.7 Cybersecurity & Sustainability

Seemingly distinct, cybersecurity and sustainability are two different features of the human condition, connected through the pervasiveness of cyberspace. At the most general level, cybersecurity may well reflect a concern for system threats to viability. Sustainability is about retaining system viability, performance, and survival.

In *CyberIR@MIT*, we situate cybersecurity and sustainability as the fourth of the system-wide domains. When we consider the various interconnections between these two features, it is not difficult to find various combinations and iterations, such as the sustainability of system cybersecurity, or cybersecurity for system sustainability.

2.2 Logic: Why *CyberIR@MIT*?

Almost every part of the world is affected by cyberspace and the “virtual.” But out approaches are ad hoc, “imported” from prevailing ideas and theories born of the “real” domain.

2.2.1 Conceptually

While everyone recognizes the salience of cyberspace, there is as yet not a shared understanding of its interconnections with various facets of human activity or diverse forms in the “real” world. This situation is especially evident in general international relations.

Mapping interconnections among the “virtual” and the “real” requires a certain degree of intellectual discipline to generate a coherent method for framing, organizing, and unbundling the diverse knowledge-content of issues central to cyberspace and international relations.

2.2.2 Strategically

Mapping the vast and seemingly incoherent knowledge arena is intended to help organize our understanding of a rapidly changing dual context, in all its forms and creative ventures. It is also designed to facilitate access to cutting-edge analysis, innovative technologies, and multidisciplinary knowledge.

2.1.1 Operationally

Framing this joint domain requires robust ways of organizing knowledge content and provision, and draws on diverse forms of expertise and interests. The result is to reduce barriers to knowledge regarding rapidly changing virtual and real situations, and to alert us when the ‘solution’ of one problem is the source of another.

2.2.3 Functionally

To the extent that the mapping "works," it provides the foundation for the design of web- based systems to enhance knowledge management, networking, and sharing, devoted to ‘sustainable development.’ This is very useful for educational purposes. It is essential to enable and/or encompass ‘voices’ from diverse perspectives.

3 Global Challenges

Before turning to the operational features of *CyberIR@MIT*—including the basics of its knowledge system, the structural elements, and the operational features—we draw upon all matters of exploration and foundation, and introduce four global challenges or issues areas. These are the domains, or issue-areas, that constitute the "subject-matter" of *CyberIR@MIT* and shape the logic for the system as a whole.

The four domains are noted below at a high level of aggregation with the understanding that each consists of highly complex features—including actors, actions, interactions, and outcomes—individually and jointly, that are near impossible to isolate from one another. These are:

1. Cyberspace & International Relations Intersections
2. Governance & Institutions
3. Conflict & War
4. Cybersecurity & Sustainability

As we move on to the knowledge system and later to the ontology, their distinctive features will become clearer, as will their interconnections. What follows is a short essay on each. Further along in this paper we elaborate on matters of knowledge, content, structure, and ontology.

3.1 Cyber-IR Intersections

We begin first with the Cyber-IR domain. The explorations leading to *CyberIR@MIT* examined the detailed features of the two arenas—cyberspace and international relations—signaling structures and processes. Given that cyberspace and the international system have been viewed as separate domains of interaction—each based on its own design principles—a joint system must first capture the basic features of each individual system and second, define the rules for their interconnections. See (Choucri & Clark, 2019).

3.1.1 Cyberspace

Defined as the virtual system enabled by Internet, the core of cyberspace. The familiar view that distinguishes between the physical infrastructure of the Internet and its role as a carrier of information, is used to frame a four-layer model. The model consists of the physical layer, the logical layer, the information layer, and the people layer.

The model is useful to describe both the technology itself, the actors that make and shape it, and the functions they perform, as well the "static" versus more "dynamic" features of each layer. Sophisticated controls at the information layer are required to address emergent international contentions.

3.1.2 International System

Defined by the traditional view of international relations framed in socially-centered hierarchical terms by familiar levels of analysis—the individual, the state, and the international system. Anchored in the principle of sovereignty, this concept defines the entities in the system.

We expand the conventional view by:

1. Defining the global system as an overarching level of analysis,
2. Extending the levels framework beyond the social domain to include *the natural environment* (life-supporting properties) and the *constructed environment* (Internet-enabled cyberspace), and
3. Recognizing the diverse forms of *system dynamics*, transformation, and change due to the construction of cyberspace and its interactions with the natural and social systems.

3.1.3 Joint Cyber-IR Domain

The Cyber-IR domain is constructed by connecting the levels of analysis in international relations and the layers of the Internet. This approach provides a view of the "whole" and the "parts" and helps contextualize actors and entities, and interests and activities, as well as sources of change and potential impacts. It is designed to identify the empirical features located at the intersection of levels and layers.

It is useful to signal that:

1. Unlike the layers structure, the permeability of influence across levels of analysis is the rule not the exception;
2. The extent to which situations and behaviors at one level influence structure and process across another varies considerably; and
3. Despite evidence of increasing cyber access worldwide, the operational norms and practices vary considerably within levels and across jurisdictions.

3.1.4 Transformation & Change

The alignment strategy of connecting the "cyber" and the "real" gives us a model within which actors and actions can be positioned and evaluated. In principle, all actors and all cyber functions can be viewed within this framework. Drawing on lateral pressure theory, we can derive some basic principles for identifying sources and consequences of transformation.

This approach yields the interconnections between foundational features of cyberspace, on the one hand, and structure and process in international relations, on the other. It should provide a full census of major actors in conjunction with the modes of interaction in their respective contexts. It will also enhance the capabilities and methods of social scientists and scholars, as well as analysts of international relations and other areas of social interaction, to understand and incorporate the larger role and character of cyberspace in diverse social contexts.

Considerable literature is already developing around these issues of transformation and change as scholars, analysts, practitioners, and policymakers seek to grapple with the new realities.

3.2 Governance & Institutions

Governance refers to the mechanisms—principles and norms, structures and processes—through which social activities are ordered, managed, and routinized over time. These are the system supporting elements of any system. For the most part, governance systems are generally formal & institutionalized in some manner, rather than entirely informal and based on norms and mutual expectations.

The international system as a whole—a system of states—is generally characterized as anarchic, conflict prone, dominated by “self-help” strategies and activities, and comparatively devoid of order—let alone law. This is the context within which the cyber domain took shape.

The governance of political systems is generally founded in some form of authority, often centralized. Governance involves organized structures and processes, legitimacy, and authority, as well as mechanisms of enforcement. This is true for individual states, for the world as a whole. There is no global government, but there are dominant norms supported by the state system.

3.2.1 Public & Private

The traditional model of government is one in which hierarchy dominates in the conduct of activities to meet responsibilities, as well as in modes and directions of accountability. The formal organizational system is also endowed with official status and assigns responsibilities to various entities within the system. Generally, consensus on norms precedes the formation of institutions. The expansion of the private sector—for profit and not-for-profit—is accompanied by the formalization of commensurate authority, often consistent with the hierarchical model.

3.2.2 Internet Governance

To simplify, governance and institutions for the cyber domain are closely connected to the design and architecture of the Internet. The core of the built ecosystems are the essential components of the Internet's architecture—Internet Technical Standards and Protocols (IP), Number Resources (ASN and IP address), and the DNS. The notion of an "ecosystem" helps to capture:

1. Critical *operational functions*
2. Embedded in specific *institutional relationships*, and
3. Organized around specific *products or processes*

The individual "parts" of the "whole" ecosystem are distinctive in their own right, as are the adjustments and applications at different levels of aggregation.

The overall architecture of *CyberIR@MIT* is framed in a global context, thus with respect to scale and scope, governance follows from the global level to international and regional processes, with the understanding that the national is contingent on the regional.

3.2.3 Functions & Capabilities

The Internet operates with institutional actors that directly perform the three major functions: technical standards, deployment, and implementation. These could be viewed as capabilities, much as we consider the capabilities of political systems.

At the same time, the construction of the Internet brought with it a distinct set of institutions—performing specific functions—that were not managed by the public sector. Over time, actors and institutions for the cyber domain evolved in different ways in relation to conventional forms of governance in the "real" domain.

3.2.4 Data & Records

In addition to the traditional forms of data collection and representation—as well as the attendant institutional and other mechanisms for the observation, collection, and measurement of information—the Cyber-IR domain harbors a wide range of added data- related processes, structures, and records. These include data regarding Internet traffic, routing and peering information, exchange points, attributes of ISP and IPS, and under networks—to note the most obvious.

3.3 Conflict & War

It goes without saying that conflict and war are ubiquitous features of the human condition—at all levels of analysis and in all contexts, everywhere. The construction of cyberspace and near-worldwide access to the Internet creates new uncertainties that are not readily accounted for by traditional understandings of conflict and war.

Here we focus less on the conventional modes of conflict—understood as a form of interaction among states—and more on the recent manifestations of cyber hostilities and intersections with traditional forms thereof. Here we characterize briefly five notable features of conflict and war, namely (1) arenas or "spaces" of conflict, (2) actors and targets, (3) threat modes and hostilities, (4) conflict dynamics, that is, manifestations and means of antagonizing & escalating, and (5) types of outcomes.

Brief, to be sure, our purpose here is only to provide a context for considering matters of structure, process, transformation, and change.

3.3.1 Conflict Systems

Traditionally, conflict and war among states takes place in a territorial context. More recently, we have begun to appreciate that humans interact within and across different "spaces" or arenas, and potentials for conflict arise accordingly. More specifically, we can delineate between four distinctive arenas of contention within which all people—states and non-states—engage in hostilities.

The four conflict systems considered here are: (a) the human system, (b) the natural system, (c) the cyber system, and (d) the intersections among them. At this point, we do not take into account outer space, only because of the limited number of actors participating therein.

3.3.2 Actors & Targets

Traditionally, we consider the key actors to be states (that is, sovereign countries with formal military capabilities), and targets to be of various types, generally kinetic in nature. For the most part, the identity of the contenders are well known. However conventional this characterization might be, it does not address today's realities nor its generative possibilities. Both actors and targets can be states as well as non-state entities, known and unknown, with or without sovereign status, using known and unknown tools directed towards known and unknown targets. All of this creates added complexity that has yet to be understood.

3.3.3 Threat & Hostilities

Whatever the underlying source of dissatisfaction, all conflicts are manifested in some threat or threat-mode. While the conventional forms are well documented and generally understood, those related or pertaining to the cyber domain—in terms of tool, weapon, strategy, damage potential, and the like—are rapidly evolving and often elusive in character and impact. The same holds for underlying motivations. Weapons and "weaponization"—usual corollaries to threats and hostility—are no longer only of the conventional kinetic type, but include uses and mal-uses of information and various types of cyber tools, to note the most obvious.

This set of issues refers to the evolution of contention, “upward escalators,” “down- ward escalators,” and various postures or strategies “in between.” There is nothing inevitable in the process, but as hostilities mount the probability of overt violence (or damage inducing actions) increases accordingly. Various strategies associated with, or designed for “de-escalation”—such as deterrence or détente, among others—are usually framed at this point, based on some assumption and associated with certain expectations.

3.3.4 Modes & Types of Outcomes

The immediate outcome of conflict and war invariably involves damages. While the nature, scale, and scope of damage varies across cases, there are some identifiable modalities. Among the most salient are damages to the wellbeing of populations, destruction of infrastructure, economic and financial damages, and damages to institutions—to note the most obvious. Also salient are environmental damages coupled with potential erosion of life-supporting properties.

The historical record also shows reconciliation and rebuilding as possible outcomes, often based on re-framing original political and other arrangements and, in more recent times, building of new institutions, national and international. Post-conflict outcomes often carry new labels to separate the past from the expected future.

3.4 Cybersecurity & Sustainability

We recognize that all systems prefer to remain sustainable. In the most general sense, sustainability is defined as:

“… the process of meeting the needs of present and future generations without undermining the resilience of the life supporting properties of nature and the integrity and security of social systems” (Choucri, 2007, p.12).

This means that we must consider sustainability in terms of ecosystems of human interactions—the social system, the natural environment, and the cyber domain. In those terms, cybersecurity is a fundamental feature of sustainability. Here we draw attention to notable features of these interconnections, with cybersecurity as the “entry point:” (a) ecosystems, actors, and activities, (b) threats and vulnerabilities, and (c) risk management and support systems.

3.4.1 Ecosystems, Actors & Activities

Consistent with the Cyber-IR logic, actors and activities are situated in different ecosystems, but their interactions result in the shaping of an overlapping and shared arena. Among the key actors are those at different layers of the Internet and different levels of analysis in international relations. Clearly, the range of activities—in layers and in levels—increases in diversity and complexity with the growth and expansion of both the cyber and the social domains.

3.4.2 Threats & Vulnerabilities

There is a catalog of threats and vulnerabilities that undermine cybersecurity and sustainability. Any listing would be outdated as soon as it is completed. Some of the recurrent themes include forms of cyber-attacks and damages, threat tools and strategies, known and unknown forms of exploitations and damages, impacts on social systems, and damages to life supporting properties—to note the obvious. The critical threshold is the point at which the loads on the system are greater than the capacity of the system to manage such loads—including threats and vulnerabilities.

3.4.3 Risk Management and System Supports

A whole range of actions are not recognized as essential for the management of risk—including social, political, technological, legal, and other(s). Risk assessments, privacy protection, system safety architecture, information security, computer network defense, and so forth are among the most salient. Human sensitivity to threat potentials, situational awareness, and social responses, as well as the development of national sustainability measures and assessment of responses all follow accordingly.

3.4.4 Resilience & Adaptation

Fundamental to the above is sustained capacity building, multi-stakeholder collaboration, institutional resilience and adaptation, and insurance and assessment measures, as well as legal and regulatory supports; all components of an overall risk management strategy. Also important are various cooperative measures at all levels of analysis, from the individual to the global.

4 What is a Knowledge System?

Webster's Collegiate Dictionary states that to "know" is to "hold something in one's mind as true or as being what it purport to be" … [This] "Implies a sound logical or factual basis." It also implies "to be convinced of." (Merriam-Webster 2020a). By extension, knowledge refers to the "fact or condition of knowing something with familiarity gained through experience or association."

4.1 Knowledge System Defined

What is 'known' is that which is 'generally recognized.' We extend this standard view of knowledge in order to take account of a cluster of understandings that we refer to as a knowledge system. We define a knowledge system as:

> *An organized structure and dynamic process to represent and generate content, components, classes or types of information, data, and forms of knowledge broadly defined.*

Conceptually, the approach to—and organization of—knowledge in *CyberIR@MIT* can best be described as an approach:

1. Characterized by domain-specific features,
2. Reinforced by a set of logical relationships that connect the content of knowledge to its value (utility),
3. Enhanced by a set of iterative processes that enable evolution, revision, and adaptation, as well as advancement, and
4. Subject to criteria of relevance, reliability & quality.

4.1.1 Architecture

The knowledge architecture of *CyberIR@MIT* is designed to represent the properties of the system segments. Technically, the knowledge architecture is designed to:

1. *Organize knowledge and data* related to each domain or issue-area into several substantive hierarchies, and related categories and subcategories into several hierarchies of interrelated sub-concepts.
2. *Define each sub-concept* of domain hierarchies to belong to a category with at least one attribute and one sub-attribute.

3. *Define the connectivity* of domain or issue categories to properties of dimensions within interrelated concepts and sub-concepts; and
4. *Provide mapping* between the data related to each of the domain hierarchies, categories, sub-categories, sub-concepts, and computer systems storing data for user functionalities.

4.1.2 Mapping

Webster's Collegiate Dictionary states that to "map" is "to represent" … "to delineate" … "to assign to every element of a …set an element of the same or another set'' and "to be located near the corresponding structural [element]." (Merriam-Webster 2020b).

Accordingly, "mapping" is the process of providing order between a property within the knowledge system and a computer for user functionalities. This is a way of representing knowledge content over areas of interest. If full knowledge changes over time, its representation must also change over time. Mapping supports:

1. *Connecting* substantive materials to the structure of hierarchies, defined as the key structures for each of the domains and dimensions,
2. *Providing* access for a plurality of entities to data within any of the sub-concepts, stored in pluralities of remote locations in response to mapping specifications,
3. *Facilitating* access to data and information in hierarchies of interrelated sub- concepts on any computer system from any sub-concept according to defined principles, and
4. *Expanding* and modifying data consistent with the structured properties of the knowledge system.

4.2 Structure & Connectivity

The knowledge architecture is applicable to a wide range of issues and problems characterized by uncertainty, complexity, and contextual diversity. This application process consists of specifying a set of interconnected, multi-dimensional relationships among actors, levels, and units.

In terms of structure, the knowledge system consists of four different aggregate macro-segments, namely:

1. *Domains*: Defining domain specific features of actors & actions
2. *Dimensions* of each domain, covering activities, as well as problems & solutions;
3. *Cells*: Representing the intersections of particular dimensions and domains;
4. *Concepts*: Referring to key sub-topics or subjects within each cell.

The knowledge architecture is integrated by a connectivity logic. This logic provides the indexing system for search and retrieval—as shown below at a conceptual level.

In Figure 2, layers refer to the dimensions of a domain, slices highlight the full dimension space for each domain; rings are the individual dimensions for each domain; and cells capture the intersection of domain and dimension at any location in the full system.

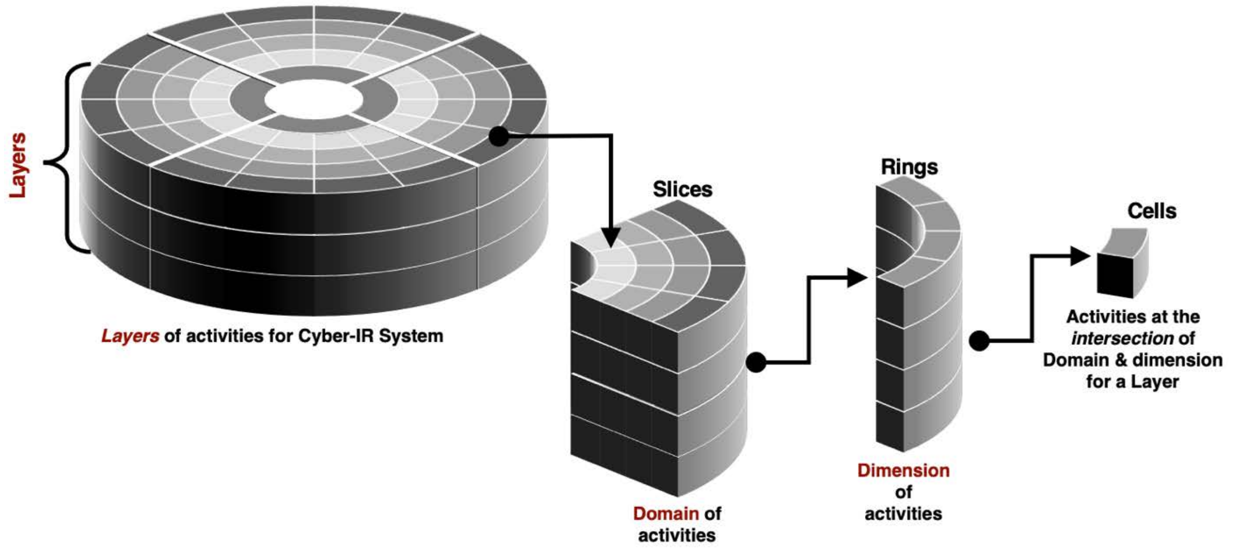

Layers
Layers of activities for Cyber-IR System
Slices
Domain of activities
Rings
Dimension of activities
Cells
Activities at the intersection of Domain & dimension for a Layer

Figure 2. Structure of knowledge architecture.

Source: Adapted from Choucri et.al. (2007).

4.2.1 Domains of Actors & Actions

The system is constructed in content-specific modules and organized into four distinct domains—as introduced earlier in Section III of this paper:

1. *Cyber-IR*, defined by layers of the Internet and levels of analysis in international relations, also includes structures, functions, and processes at the intersection of the two areas.
2. *Governance & Institutions*, represent the operational features of authority systems with supportive properties and mechanisms designed to stabilize structures and functions embedded in and surrounding the Cyber-IR domain.

3. *Conflict & War*, captures system-threats, spanning the sources and consequences of multiple pressures that undermine the security and resilience of the joint Cyber-IR system whole or parts.
4. *Cybersecurity & Sustainability*, captures cyber-driven threats, modes of response & their various features, as well as the support for and threats to system stability & resilience over time.

   These are shown in Figure 3 below.

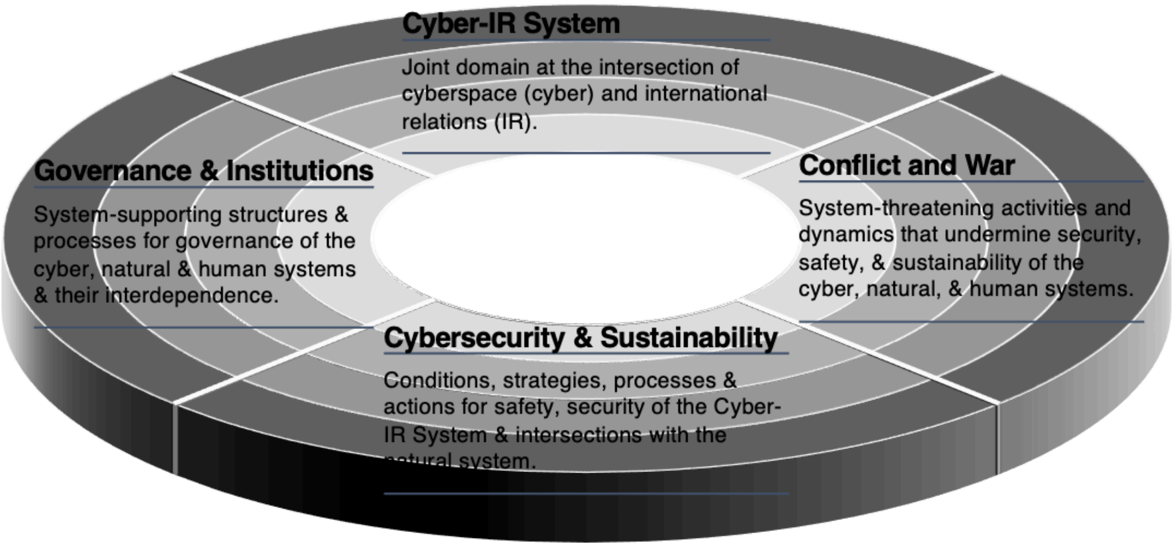

Cyber-IR System
Joint domain at the intersection of cyberspace (cyber) and international relations (IR).
Governance & Institutions
System-supporting structures & processes for governance of the cyber, natural & human systems & their interdependence.
Conflict and War
System-threatening activities and dynamics that undermine security, safety, & sustainability of the cyber, natural, & human systems.
Cybersecurity & Sustainability
Conditions, strategies, processes & actions for safety, security of the Cyber-IR System & intersections with the natural system.

Figure 3. Domains of actors & actions.

4.2.2 Dimensions of Actors & Actions

Each domain is framed and differentiated in terms of four characteristic features, each distinctive in its own right:

1. *System State*—characteristic features and properties of the domain in its "as is" state.
2. *System Problems*—manifestations of recognized, anticipated, simulated, or other aspects of problems surrounding or embedded in the system state.
3. *Scientific & Technological Solutions & Strategies*—including formal and informal efforts, initiatives, regulations, and policies created in response to system problems.

4. *Socio-Economic & Political Solutions & Strategies*—including formal and informal efforts, initiatives, regulations, and policies created in response to system problems.

   These are shown in Figure 4 below.

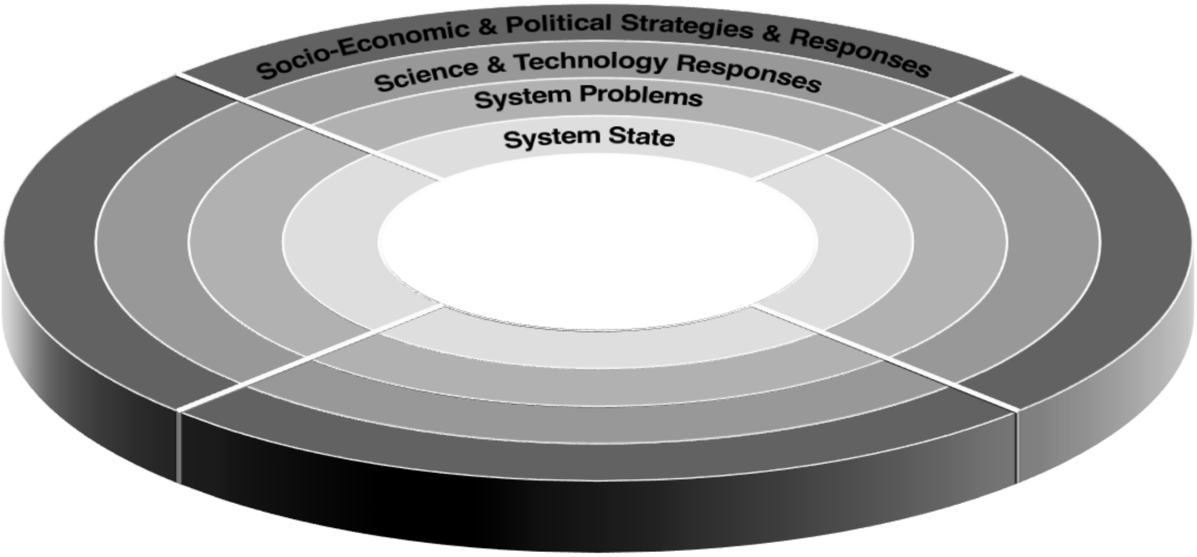

Socio-Economic & Political Strategies & Responses
Science & Technology Responses
System Problems
System State

Figure 4. Dimensions of actors & actions.

4.2.3 Intersections

The intersection is the content of the knowledge "space" at the juncture of individual domains and dimensions. Intersections provide access to more focused or detailed knowledge about system properties.

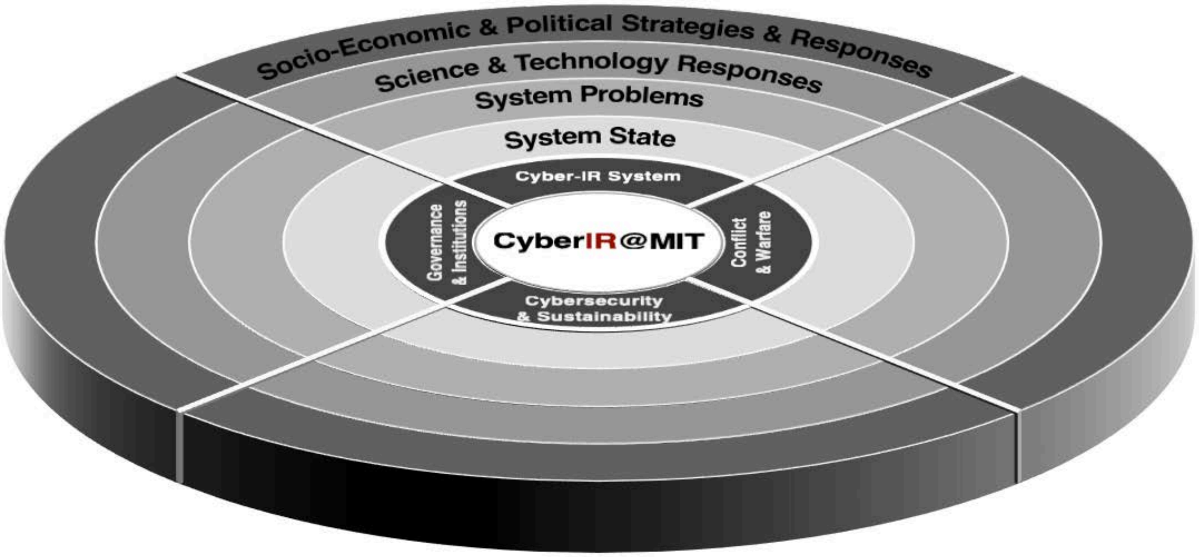

Socio-Economic & Political Strategies & Responses
Science & Technology Responses
System Problems
System State
Cyber-IR System
Governance & Institutions
CyberIR@MIT
Conflict & Warfare
Cybersecurity & Sustainability

Figure 5. Intersection of domain and dimension.

Note that Figures 2 to 5 are simplified for representation purposes only. This means that each Figure is “flattened” and does not provide an accurate reflection of the relationship between domains and dimensions. By the same token, it does not signal the depth of knowledge content for the domains or dimensions.

We shall return to this issue later in the paper by providing a “correction” for this “flattened” representation.

5 High-Level View for Knowledge System of *CyberIR@MIT*

At this point we present a high-level aggregation of knowledge for *CyberIR@MIT*—in terms of domains and dimensions for each content segment in the system. What follows is a highly simplified representation of each domain, largely for orientation purposes.

1. *Cyber-IR Domain*, defined as the intersection of international relations and cyberspace and consists of the key layers of the Internet and the levels of analysis in international relations—and their intersection.
2. *Governance & Institutions*, represents the supportive properties and mechanisms that buttress the Cyber-IR reality. These mechanisms of governance are designed to stabilize societies.
3. *Conflict & War*, captures the multiple pressures and threats that can result in social damage & fundamental destruction.
4. *Cybersecurity & Sustainability* captures cyber-driven threats to, & support for, system stability & resilience, modes of response and their various features, as well as propensities for sustainability and strategies for sustainable development.

The ontology is rooted in research and results reported in *Cyberpolitics in International Relations* (Choucri, 2012) and *International Relations in the Cyber Age: The Co- Evolution Dilemma* (Choucri & Clark, 2019)—as well as the results in “Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review” (Ramirez & Choucri, 2016).

We now turn each domain and present a high-level view of the contents. The website hosts a detailed view of each domain. While “the devil is in the details” as is often said, the website provides sufficient details to ward off the “devil.”

5.1 Cyber-IR Domain

Defined as the “space” at the intersection of international relations and cyberspace, this domain, shown in Figure 6, consists of the key layers of the Internet and the levels of analysis in international relations—their intersection, and their interactions. (In this and following figures, blank entries indicate content under review).

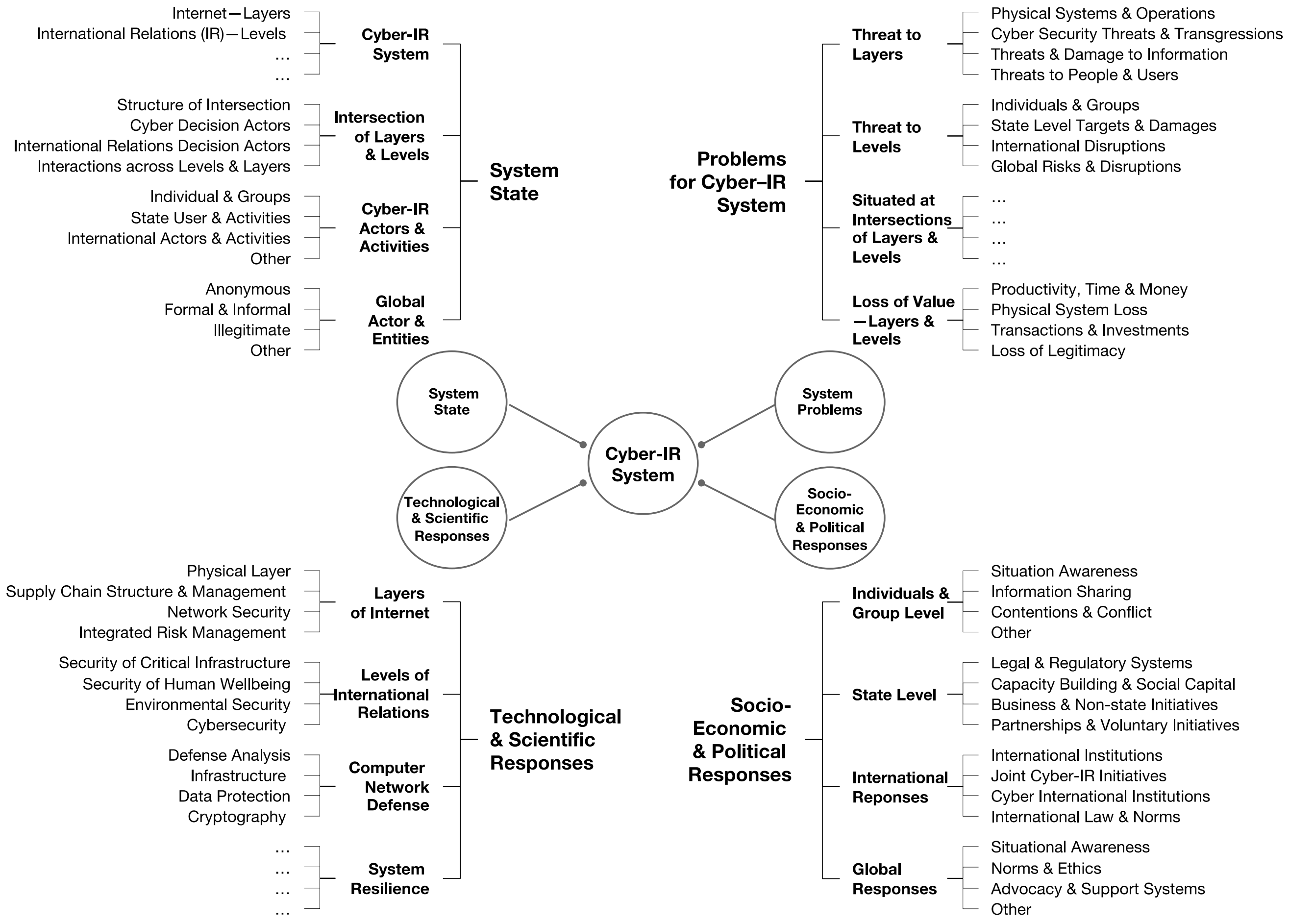

Internet—Layers
International Relations (IR)—Levels
…
…
Cyber-IR System
Structure of Intersection
Cyber Decision Actors
International Relations Decision Actors
Interactions across Levels & Layers
Intersection of Layers & Levels
Individual & Groups
State User & Activities
International Actors & Activities
Other
Cyber-IR Actors & Activities
Anonymous
Formal & Informal
Illegitimate
Other
Global Actor & Entities
System State
Problems for Cyber–IR System
Threat to Layers
Physical Systems & Operations
Cyber Security Threats & Transgressions
Threats & Damage to Information
Threats to People & Users
Threat to Levels
Individuals & Groups
State Level Targets & Damages
International Disruptions
Global Risks & Disruptions
Situated at Intersections of Layers & Levels
…
…
…
…
Loss of Value —Layers & Levels
Productivity, Time & Money
Physical System Loss
Transactions & Investments
Loss of Legitimacy
System State
System Problems
Cyber-IR System
Technological & Scientific Responses
Socio-Economic & Political Responses
Physical Layer
Supply Chain Structure & Management
Network Security
Integrated Risk Management
Layers of Internet
Security of Critical Infrastructure
Security of Human Wellbeing
Environmental Security
Cybersecurity
Levels of International Relations
Defense Analysis
Infrastructure
Data Protection
Cryptography
Computer Network Defense
…
…
…
…
System Resilience
Technological & Scientific Responses
Socio-Economic & Political Responses
Individuals & Group Level
Situation Awareness
Information Sharing
Contentions & Conflict
Other
State Level
Legal & Regulatory Systems
Capacity Building & Social Capital
Business & Non-state Initiatives
Partnerships & Voluntary Initiatives
International Reponses
International Institutions
Joint Cyber-IR Initiatives
Cyber International Institutions
International Law & Norms
Global Responses
Situational Awareness
Norms & Ethics
Advocacy & Support Systems
Other

Figure 6. High-level ontology for *Cyber-IR* domain.

5.2 Governance & Institutions

The domain represents the supportive properties and mechanisms of governance that buttress the Cyber-IR systems and related realities. These mechanisms are designed to stabilize—and to enable and support—societies.

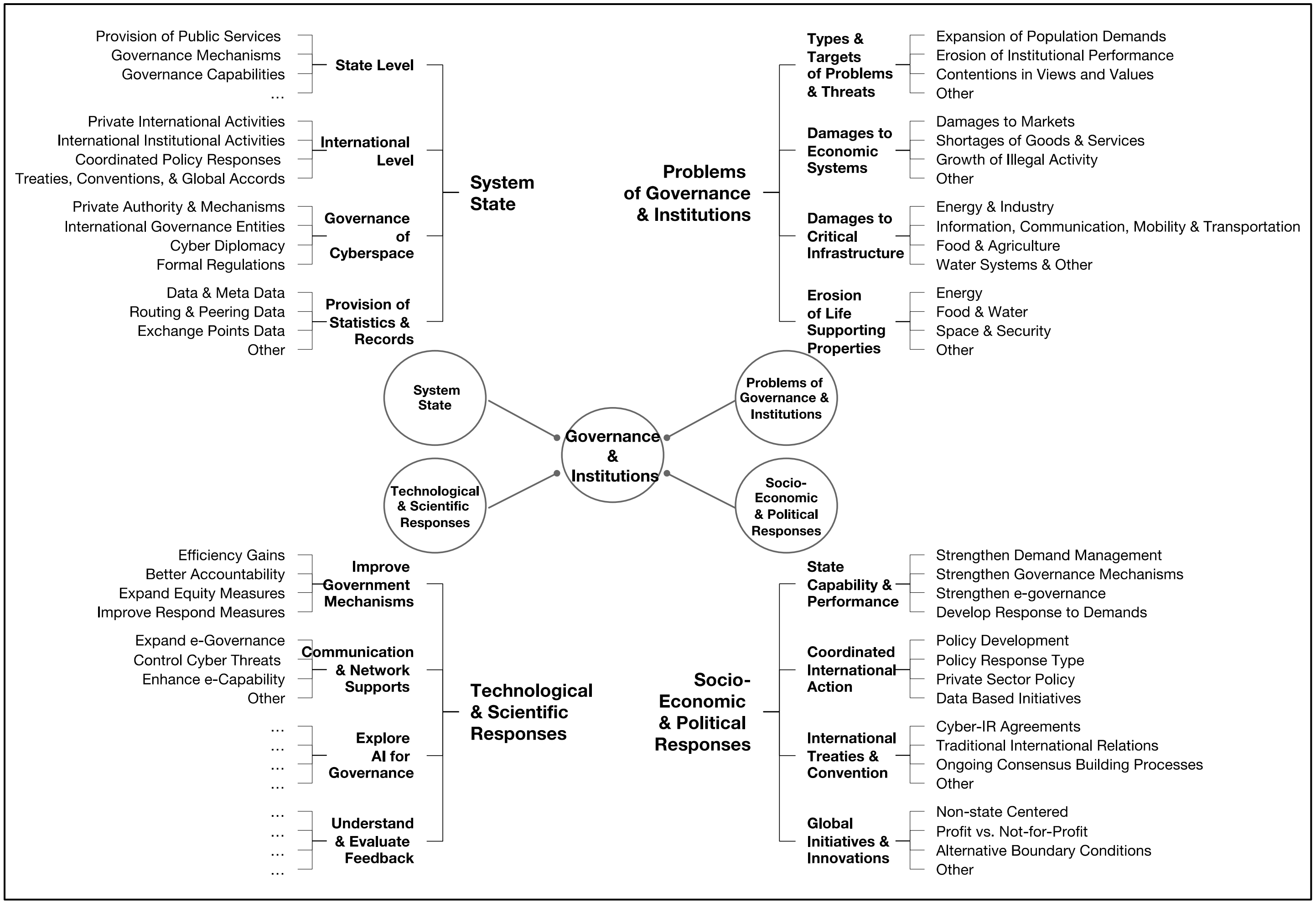

Governance & Institutions
System State
Problems of Governance & Institutions
Technological & Scientific Responses
Socio-Economic & Political Responses
State Level
Provision of Public Services
Governance Mechanisms
Governance Capabilities
…
International Level
Private International Activities
International Institutional Activities
Coordinated Policy Responses
Treaties, Conventions, & Global Accords
Governance of Cyberspace
Private Authority & Mechanisms
International Governance Entities
Cyber Diplomacy
Formal Regulations
Provision of Statistics & Records
Data & Meta Data
Routing & Peering Data
Exchange Points Data
Other
Types & Targets of Problems & Threats
Expansion of Population Demands
Erosion of Institutional Performance
Contentions in Views and Values
Other
Damages to Economic Systems
Damages to Markets
Shortages of Goods & Services
Growth of Illegal Activity
Other
Damages to Critical Infrastructure
Energy & Industry
Information, Communication, Mobility & Transportation
Food & Agriculture
Water Systems & Other
Erosion of Life Supporting Properties
Energy
Food & Water
Space & Security
Other
Improve Government Mechanisms
Efficiency Gains
Better Accountability
Expand Equity Measures
Improve Respond Measures
Communication & Network Supports
Expand e-Governance
Control Cyber Threats
Enhance e-Capability
Other
Explore AI for Governance
…
…
…
…
Understand & Evaluate Feedback
…
…
…
…
State Capability & Performance
Strengthen Demand Management
Strengthen Governance Mechanisms
Strengthen e-governance
Develop Response to Demands
Coordinated International Action
Policy Development
Policy Response Type
Private Sector Policy
Data Based Initiatives
International Treaties & Convention
Cyber-IR Agreements
Traditional International Relations
Ongoing Consensus Building Processes
Other
Global Initiatives & Innovations
Non-state Centered
Profit vs. Not-for-Profit
Alternative Boundary Conditions
Other

Figure 7. High-level ontology for *Governance & Institutions* domain.

5.3 Conflict & War

The domain of conflict and war captures the multiple pressures and threats that can result in social damage & fundamental destruction.

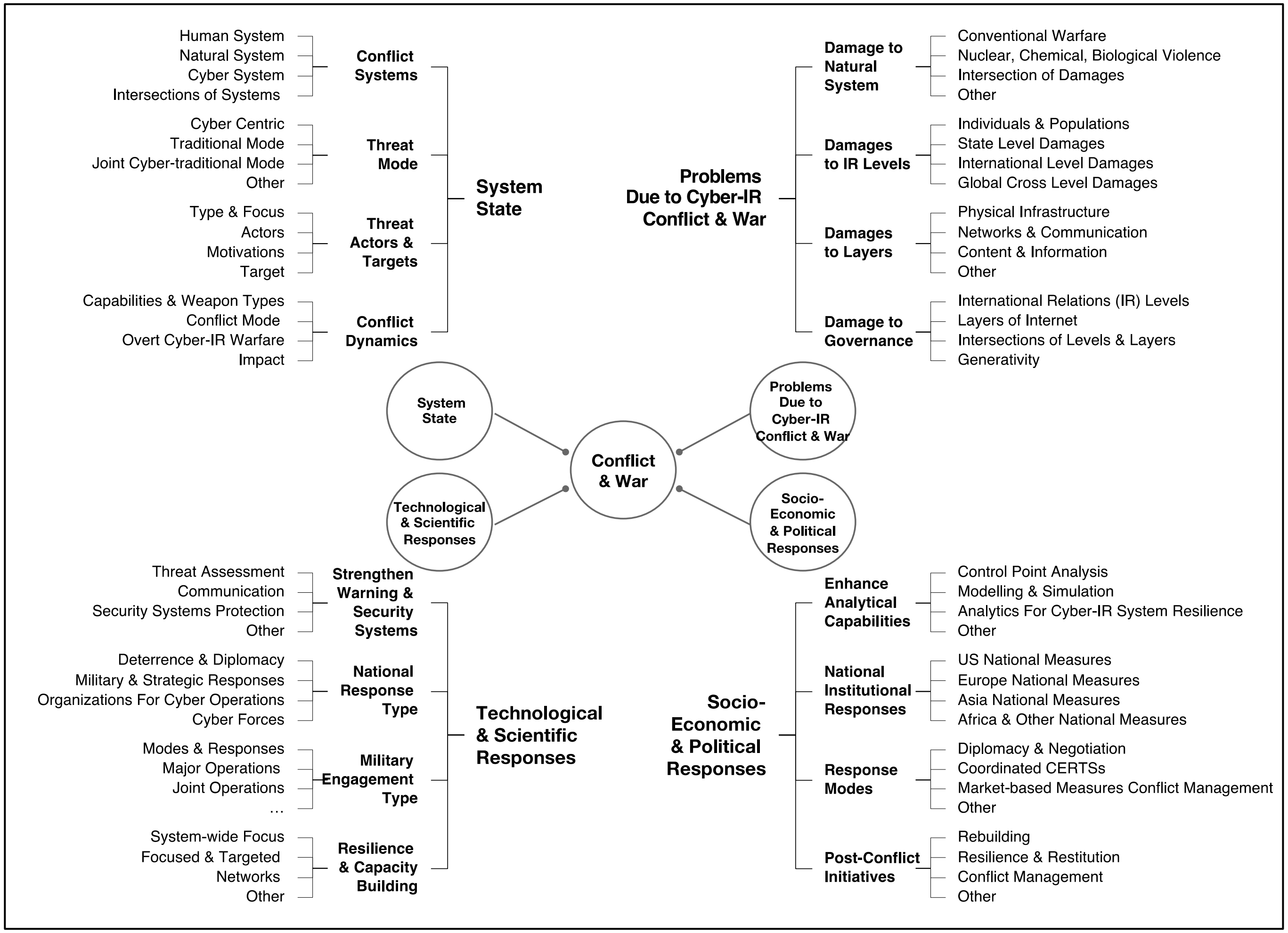
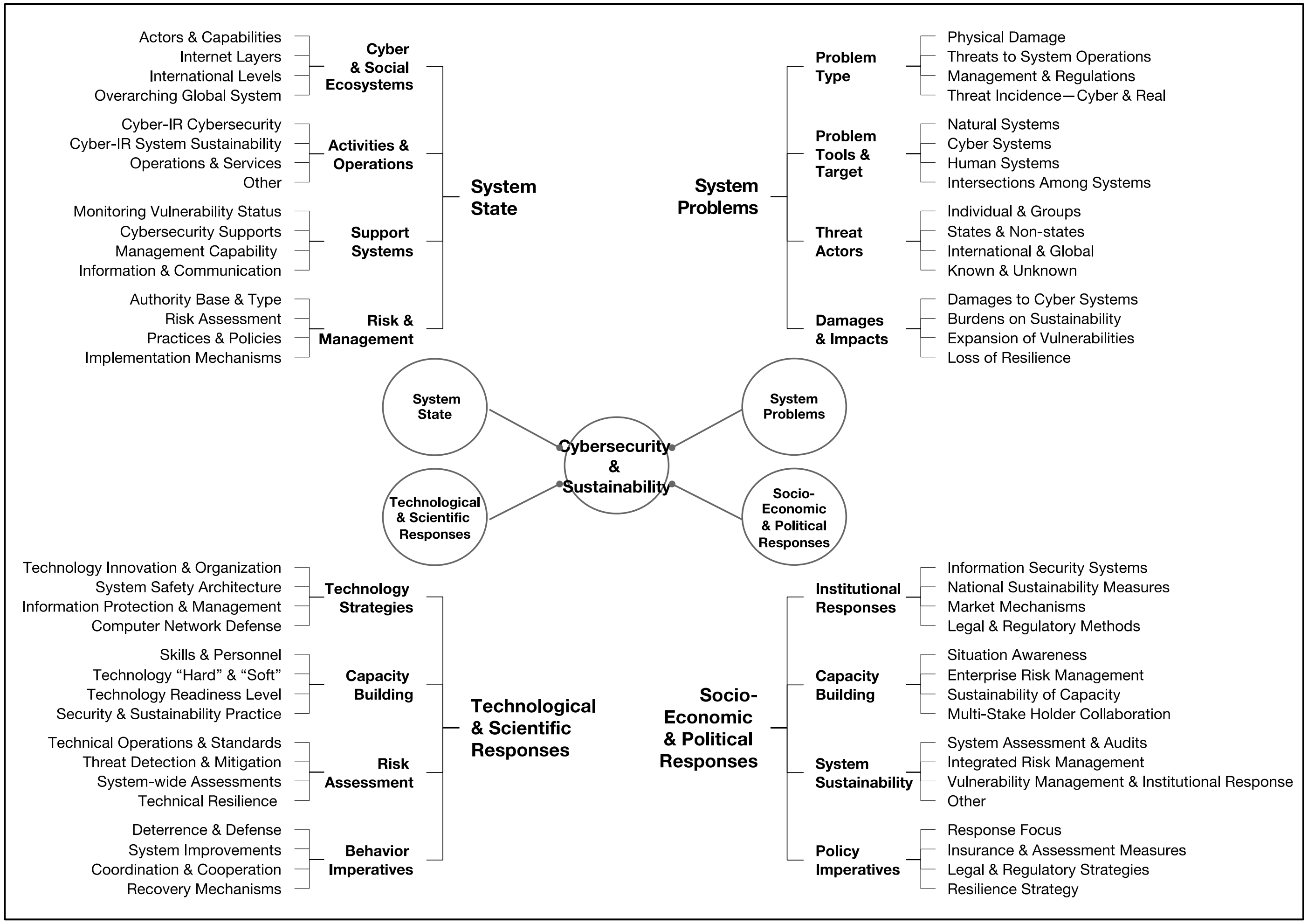


Figure 8. High-level ontology for *Conflict & War* domain.

5.4 Cybersecurity & Sustainability

This domain captures cyber-driven threats to & support for system stability & resilience over time, modes of response & their various features, as well as propensities for sustainability and strategies for sustainable development.



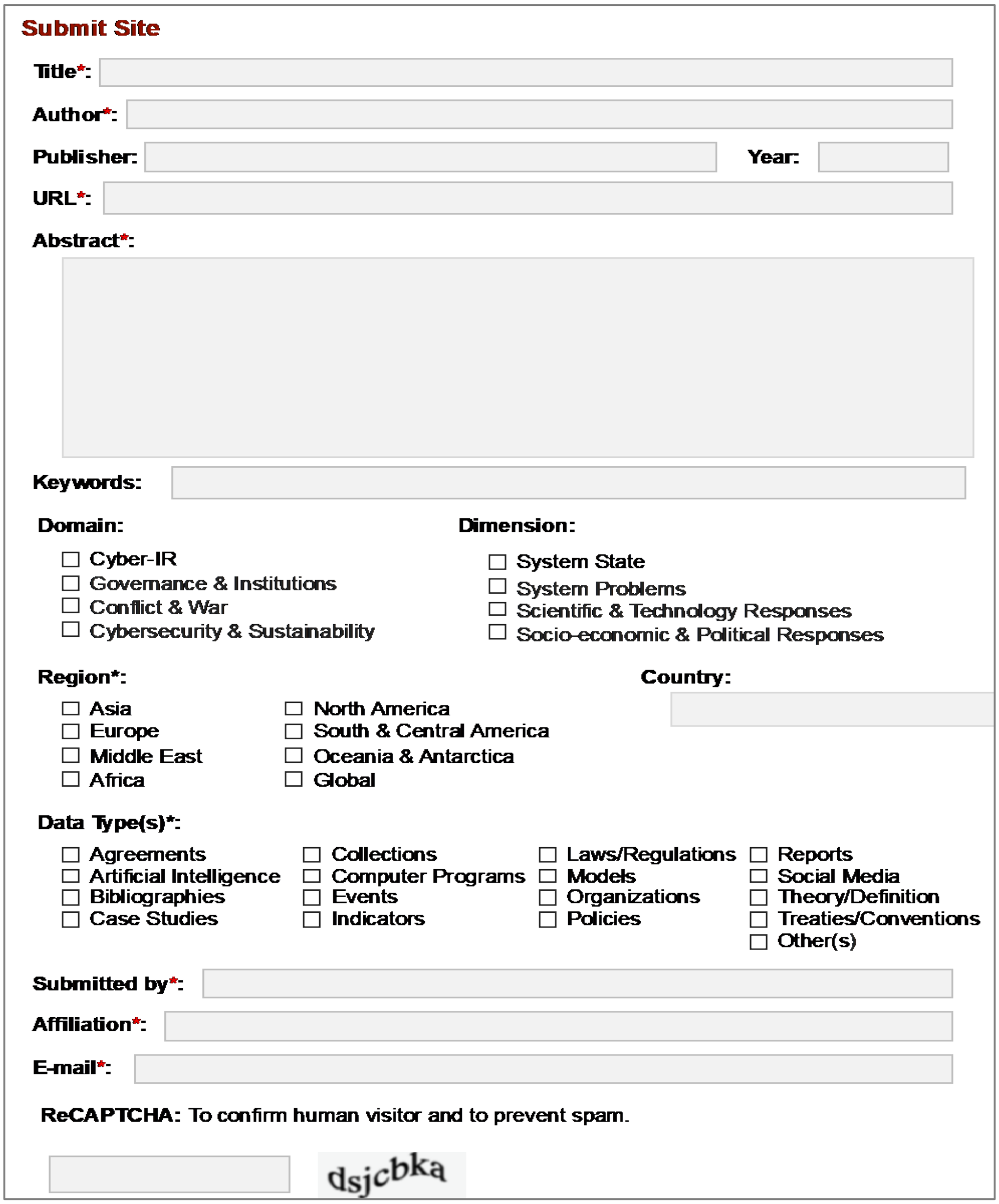
Actors & Capabilities
Internet Layers
International Levels
Overarching Global System
Cyber & Social Ecosystems
Cyber-IR Cybersecurity
Cyber-IR System Sustainability
Operations & Services
Other
Activities & Operations
Monitoring Vulnerability Status
Cybersecurity Supports
Management Capability
Information & Communication
Support Systems
Authority Base & Type
Risk Assessment
Practices & Policies
Implementation Mechanisms
Risk & Management
System State
Problem Type
Physical Damage
Threats to System Operations
Management & Regulations
Threat Incidence—Cyber & Real
Problem Tools & Target
Natural Systems
Cyber Systems
Human Systems
Intersections Among Systems
Threat Actors
Individual & Groups
States & Non-states
International & Global
Known & Unknown
Damages & Impacts
Damages to Cyber Systems
Burdens on Sustainability
Expansion of Vulnerabilities
Loss of Resilience
System Problems
System State
System Problems
Cybersecurity & Sustainability
Technological & Scientific Responses
Socio-Economic & Political Responses
Technology Innovation & Organization
System Safety Architecture
Information Protection & Management
Computer Network Defense
Technology Strategies
Skills & Personnel
Technology "Hard" & "Soft"
Technology Readiness Level
Security & Sustainability Practice
Capacity Building
Technical Operations & Standards
Threat Detection & Mitigation
System-wide Assessments
Technical Resilience
Risk Assessment
Deterrence & Defense
System Improvements
Coordination & Cooperation
Recovery Mechanisms
Behavior Imperatives
Technological & Scientific Responses
Socio-Economic & Political Responses
Institutional Responses
Information Security Systems
National Sustainability Measures
Market Mechanisms
Legal & Regulatory Methods
Capacity Building
Situation Awareness
Enterprise Risk Management
Sustainability of Capacity
Multi-Stake Holder Collaboration
System Sustainability
System Assessment & Audits
Integrated Risk Management
Vulnerability Management & Institutional Response
Other
Policy Imperatives
Response Focus
Insurance & Assessment Measures
Legal & Regulatory Strategies
Resilience Strategy

Figure 9. High-level ontology for *Cybersecurity & Sustainability* domain.

The remainder of this paper addresses operational issues, and introduces the user to the formats for knowledge provision, and for search and retrieval over the evolving Cyber-IR knowledge base

6 Knowledge Provision: Submit Site

The “Submit Site” and “Search *CyberIR@MIT*” functions are core functions for the user needs. Below is the protocol for submission, useful also for cross reference. Each submission is reviewed for integrity before it is included into the database.



Submit Site

Title*:

Author*:

Publisher: **Year:**

URL*:

Abstract*:

Keywords:

Domain:

- □ Cyber-IR
- □ Governance & Institutions
- □ Conflict & War
- □ Cybersecurity & Sustainability

Dimension:

- □ System State
- □ System Problems
- □ Scientific & Technology Responses
- □ Socio-economic & Political Responses

Region*:

- □ Asia
- □ Europe
- □ Middle East
- □ Africa
- □ North America
- □ South & Central America
- □ Oceania & Antarctica
- □ Global

Country:

Data Type(s)*:

- □ Agreements
- □ Artificial Intelligence
- □ Bibliographies
- □ Case Studies
- □ Collections
- □ Computer Programs
- □ Events
- □ Indicators
- □ Laws/Regulations
- □ Models
- □ Organizations
- □ Policies
- □ Reports
- □ Social Media
- □ Theory/Definition
- □ Treaties/Conventions
- □ Other(s)

Submitted by*:

Affiliation*:

E-mail*:

ReCAPTCHA: To confirm human visitor and to prevent spam.

dsjcbka

Figure 10. Sample submit webform.

7 Search Options

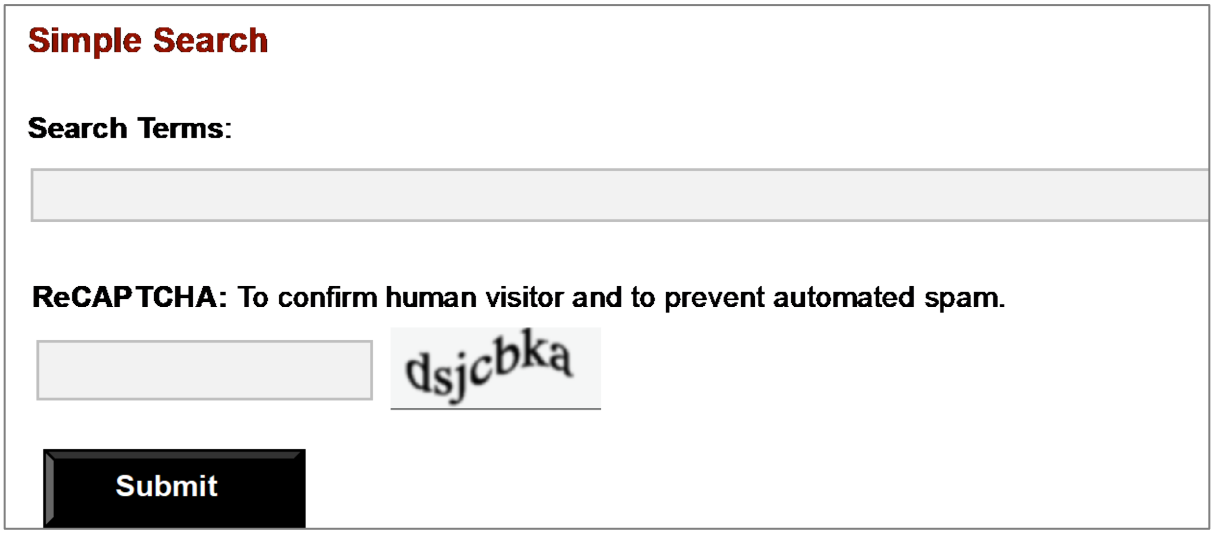
Navigation and search mechanisms operate over the *CyberIR@MIT* knowledge base. Recall that the knowledge base itself is initially generated through the screening and selection of quality and integrity. *CyberIR@MIT* provides two text-based search options and three graphic navigation options.

7.1 Text-based Options

Text-based options consist of simple and advanced protocols.

7.1.1 Simple Search

User-defined text search (e.g., China, energy, population) is entered in the following web form:

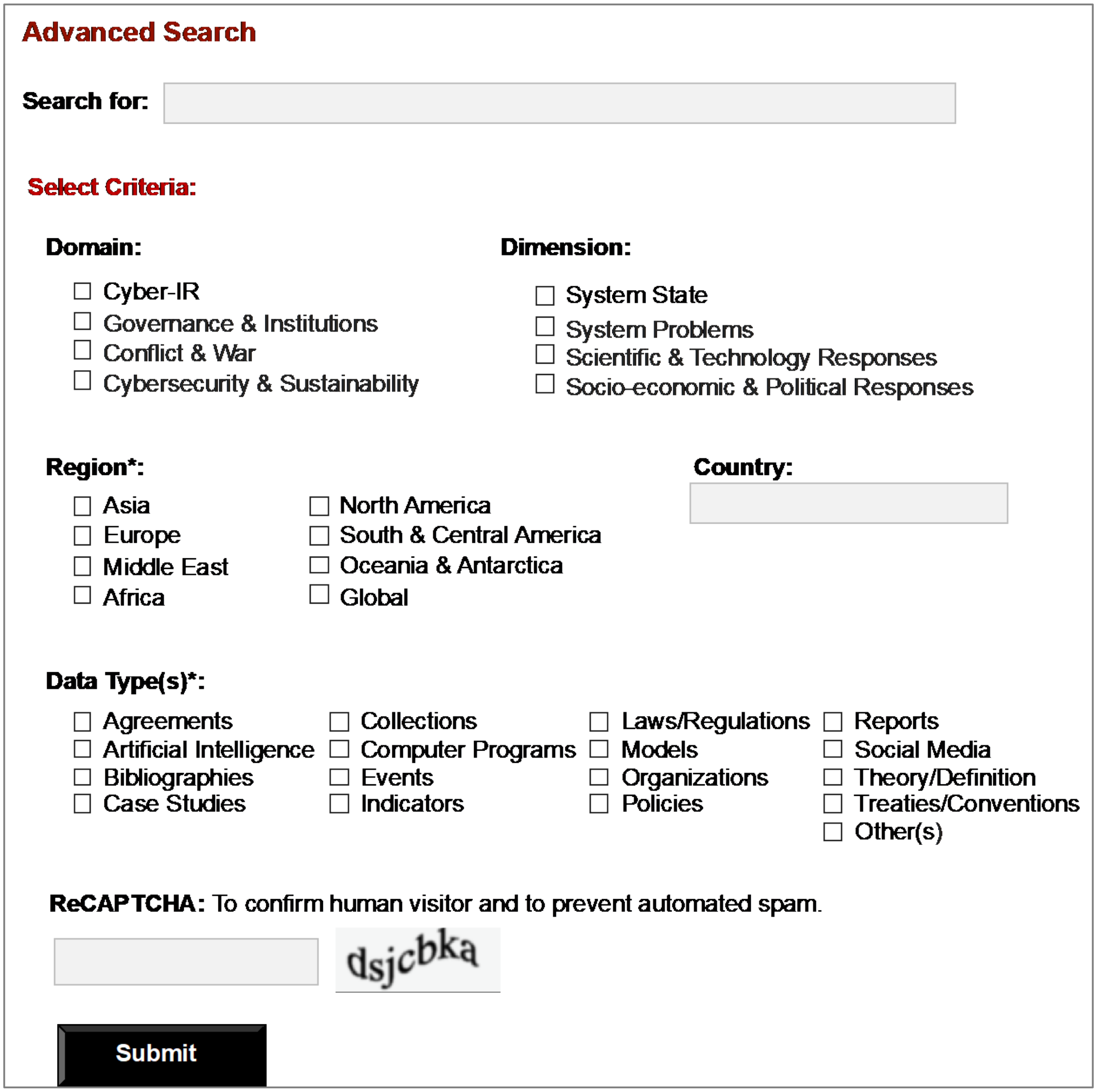


ReCAPTCHA: To confirm human visitor and to prevent automated spam.

Figure 11. Simple search form.

7.1.2 Advanced Search

Advanced search is based in a protocol that captures search criteria by domain, dimension, region, country, and data type. This option enables a more refined request for data.



Advanced Search

Search for:

Select Criteria:

Domain:

□ Cyber-IR
□ Governance & Institutions
□ Conflict & War
□ Cybersecurity & Sustainability

Dimension:

□ System State
□ System Problems
□ Scientific & Technology Responses
□ Socio-economic & Political Responses

Region*:

□ Asia
□ Europe
□ Middle East
□ Africa
□ North America
□ South & Central America
□ Oceania & Antarctica
□ Global

Country:

Data Type(s)*:

□ Agreements
□ Artificial Intelligence
□ Bibliographies
□ Case Studies
□ Collections
□ Computer Programs
□ Events
□ Indicators
□ Laws/Regulations
□ Models
□ Organizations
□ Policies
□ Reports
□ Social Media
□ Theory/Definition
□ Treaties/Conventions
□ Other(s)

ReCAPTCHA: To confirm human visitor and to prevent automated spam.

dsjcbka

Submit

Figure 12. Advanced search form.

7.2 Graphic Options

Graphic search options follow the same general structure of the knowledge base by enabling searches by domain, dimension, and the intersection of the two. (To be implemented).

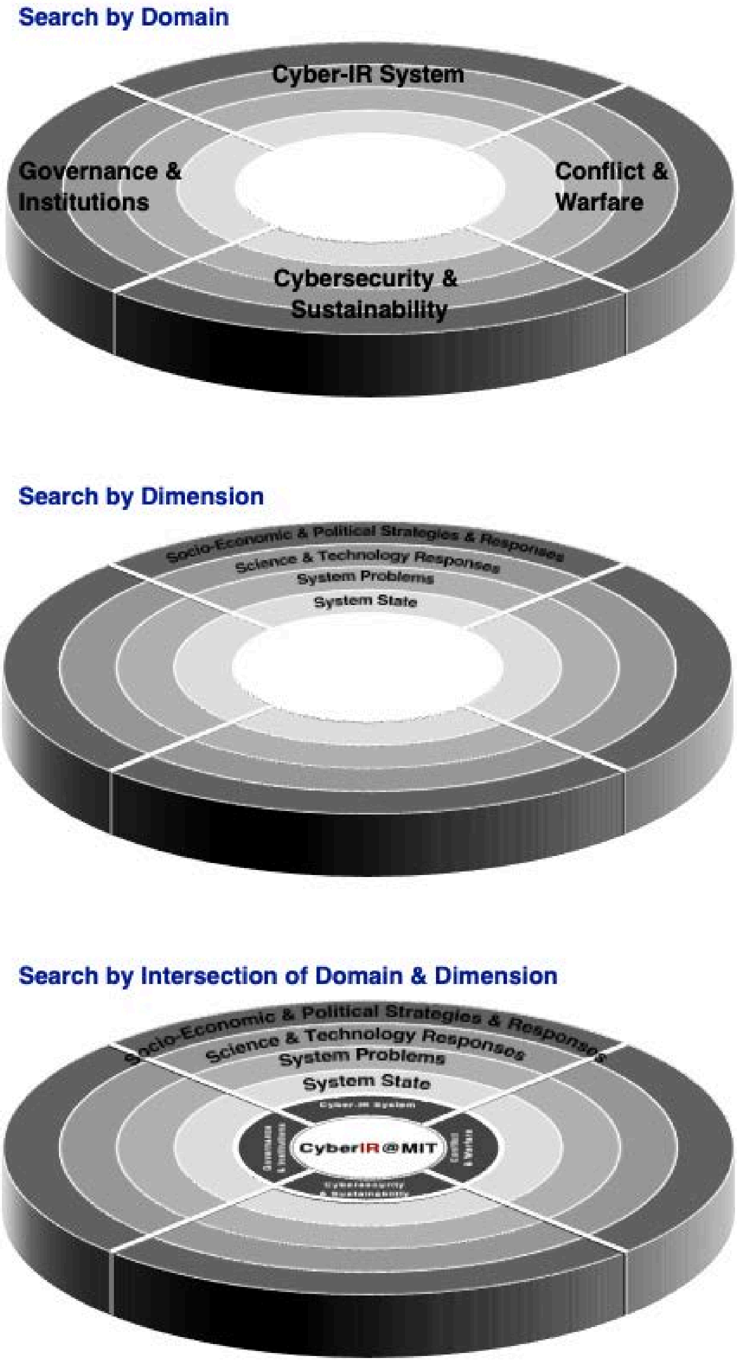

Search by Domain
Cyber-IR System
Governance & Institutions
Conflict & Warfare
Cybersecurity & Sustainability
Search by Dimension
Socio-Economic & Political Strategies & Responses
Science & Technology Responses
System Problems
System State
Search by Intersection of Domain & Dimension
Socio-Economic & Political Strategies & Responses
Science & Technology Responses
System Problems
System State
Cyber-IR System
Cybersecurity & Sustainability
CyberIR@MIT

Figure 13. Graphic search form.

8 End Note

As noted earlier, the value proposition of *CyberIR@MIT* lies in (1) conceptual foundations, (2) knowledge system or ontology, (3) distributed user submissions to the knowledge base and (4) use of different search options.

The system as a whole—especially the articulation and representation of knowledge—focuses on the intersection of cyberspace and international relations, and requires the differentiation of central features for each of these areas or "spaces."

The domain of *Cyber-IR* recognizes the situational contexts of Cyber-IR, and therefore articulates the knowledge content of critical interconnections between the two "spaces."

Governance & Institutions represent the system-supporting functions and capabilities of society.

Conflict & War capture the system threats that undermine stability and security.

Cybersecurity & Sustainability span complex dynamics. The first term covers specific cyber-international relations security-related issues. The second term addresses key imperatives for security, safety, resilience and stability of social, cyber, and natural systems.

As structured, *CyberIR@MIT* can be relevant to different types of "users"—ranging from those that "demand" knowledge and information on select issues of interest to those that seek to "supply" knowledge to a broader community.

A review process for "quality" is designed to verify the sources provided for the data base and the integrity of knowledge provision. The knowledge representation methods and processes of knowledge provision have been "tested" in the course of the MIT-Harvard Project *Explorations in Cyber International Relations.*

9 Select References

9.1 Publications

1. Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge MA: MIT Press.

2. Choucri, Nazli. 2016. "Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University." *MIT Political Science Department Research Paper* No. 2016-1, Cambridge, MA: Massachusetts Institute of Technology. http://dx.doi.org/10.2139/ssrn.2727414).

3. Choucri, Nazli, and David D. Clark. 2019. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge MA: MIT Press.

4. Choucri, Nazli, Dinsha Mistree, Farnaz Haghseta, Toufic Mezher, Wallace R. Baker, Carlos I. Ortiz. 2007. *Mapping Sustainability: e-Networking & and Value Chain*. Dordrecht, Netherlands: Springer.

5. Merriam-Webster. 2020a. *Know*. https://www.merriam-webster.com/dictionary/know.

6. Merriam-Webster. 2020b. *Map*. https://www.merriam-webster.com/dictionary/map.

7. Ramirez, Robert, and Choucri N. 2016. "Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review", *IEEE Access*, 2216–2223.

9.2 Websites

1. CyberIR@MIT. 2021. https://cyberir.mit.edu

2. *Exploration in Cyber International Relations* (ECIR). 2021. http://ecir.mit.edu/.

3. *Global System for Sustainable Development* (GSSD). 2021. http://gssd.mit.edu.