International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 11

Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms

Claire Vishik, Mihoko Matsubara, Audrey Plonk

1. Introduction

1.1 Definition of Cyber Security

Cyber security is a complex subject and has a number of definitions, such as this from the National Initiative for Cyber Security Careers and Studies (NICCS):

> 'The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.'[1]

The same source also offers an extended definition:

> 'Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military,

1 NICCS, 'Explore Terms: A Glossary of Common Cybersecurity Terminology,' https://niccs.us-cert.gov/glossary.

and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.'[2]

1.2 Multidisciplinary Context for Cyber Security Norms

In this chapter, we do not attempt to offer a comprehensive analysis of various cyber security contexts, but rather to compare common elements in a set of representative documents and explore the connection between shared principles and domain-specific norms in a context that encompasses policy, technology, and societal issues.

The white paper adopted by several industry associations in Europe, Asia, and the US, entitled *Moving Forward Together: Recommended Industry and Government Approaches to the Continued Growth and Security of Cyberspace,* observes: 'Technology and services change and evolve rapidly, and policymaking related to cyberspace must also be innovative to support growth, security, trust and confidence, and stability'. All stakeholders (government, industry, academia, and civil society) must work together to ensure that the benefits of cyberspace are accessible to citizens, and that major challenges are addressed.[3] While a government is responsible for developing policies, strategies, and regulatory conditions for the development of cyber security, industry is the source of cutting-edge technologies, technical expertise, deployment and operational experience, and, in many countries, owns major components of critical infrastructure. Multi-stakeholder cooperation requires a common context to enable the participants to collaborate constructively. Industry owns and operates a significant part of the Internet infrastructure and develops and deploys technologies responsible for the operations and evolution of cyberspace. For both industry and government, the shared context is important because it permits regulators to design policies consistent with the technology space and flows of information and allows industry to introduce products and solutions that are aligned with high-level principles and based on specific norms and best practices. A richer context proposed in this paper could explain, for example, why an implementation of a network service is compliant with generally accepted privacy requirements, and what best practices and technology norms, such as the use of privacy-preserving cryptographic protocols, have been employed to achieve these goals. In another example, rich context can provide practical guidance on solutions available to increase the reach of cyberspace to areas with limited infrastructure based on the standards and technologies available today. The need for the shared context in cyber security and challenges associated with its creation are also highlighted in research.[4]

2 Ibid.

3 'Moving Forward Together: Recommended Industry and Government Approaches for the Continued Growth and Security of Cyberspace' (*BSA* | The Software Alliance, et al, Seoul Conference on Cyberspace 2013, October 2013), 1-2, http://www.itic.org/dotAsset/9/d/9dede1e6-0281-4c19-84c5-00b8209b7bea.pdf. Adopted by five industry associations in conjunction with the Cyber Space Conference in Seoul in 2013.

4 Jeffrey Hunker, 'Policy Challenges in Building Dependability in Global Infrastructures,' *Computers & Security* 21 (2002): 705-711; Bruce L. Benson, 'The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement without the State,' *Journal of Law, Economics and Policy* 269 (2005).

There are a number of multi-disciplinary principles or guidelines that should be approached as a whole, to ensure that societal, policy, and technology aspects are integrated; this is illustrated in Table 1, which is based on the example offered by OECD Guidelines for cyber security.

Table 1. Nine Principles from the OECD Guidelines.[5]

Type of Elements	Principles	Description
Policy, organisational	Awareness	Needs and requirements for security of information systems and benefits of their implementation should be recognised
	Responsibility	Responsibility for the security of information systems and networks should be shared by all
	Response	Timely and co-operative way to prevent, detect and respond to security incidents is necessary
Technology	Risk assessment	Regular structured risk assessments should be conducted
	Security design and implementation	Security should be incorporated as an essential element of information systems and networks
	Security management	A comprehensive approach to security management should be adopted
	Reassessment	Appropriate modifications to security policies, practices, measures and procedures should be made as the environment changes
Societal	Ethics	Legitimate interests of others should be respected; work should be conducted in an ethical manner
	Democracy	The security of information systems and networks should be compatible with essential values of a democratic society

While the development of high level concepts and guidelines has been relatively successful, it has proved a challenge to define a multi-disciplinary integrated model that could allow technologists and policy-makers to easily collaborate on developing viable cyber security policies and approaches to cyber norms that are compatible with a quickly evolving technology environment. The global nature of the Internet and the ubiquitous use of cyberspace worldwide require the amalgamation of various disciplines and the collaboration of academia, government, industry, and civil society organisations. However, the research and practitioners community has not developed a mechanism to link more concrete and frequently domain-specific norms to the high-level principles in a scientific and predictable fashion.

The lack of a rich common context, comprising both principles and norms, has delayed the emergence of harmonised mechanisms which would enable the multi-stakeholder community to build on the shared values associated with the societal, policy, and technological aspects of cyber security. It has also led to weaknesses in the technology space, where policy requirements are not always adequately incorporated, and in policy design, where technology constraints are not always well understood.

5 'OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security' (Organization for Economic Co-operation and Development, 25 July 2002), 10-12, http://www.oecd.org/sti/ieconomy/15582260.pdf.

1.3 Principles and Norms

As the article focuses on establishing a common context, it is necessary to use broad, all-encompassing definitions. A norm is simply defined as a standard, model or pattern, in reference to technology norms and best practices discussed in this chapter. These norms are based on high-level principles, defined as basic truths, theories or ideas that form a basis of something.[6] This chapter discusses policy principles. Multi-stakeholder groups frequently focus on the development of principles because the high level of generalisation permits diverse participants to form convergent views. Norms, especially technical norms, are more frequently defined by communities with specialised knowledge and expertise. Although efforts are made to design technical norms and best practices based on accepted policy principles, the link between the norms and the principles and between the technology and the policy space is highly abstract. This level of abstraction simplifies consensus, but also complicates discussions on design and implementations of cyber security policies that take into consideration both norms and principles.

The typical (and constructive) approach in multi-stakeholder efforts in cyber security is to propose common high-level policy principles and to ensure that the technical norms are developed in accordance with them. This top-down view leads to positive results for agreeing on industry norms. An example of such consensus achieved on high-level principles in a complicated area is the encryption principles developed by the World Semiconductor Council.[7] However, this approach is not always sufficient for the incorporation of the requirements defined by the technology space and technology constraints into the policy design process. The limitations are due in part to the complexity and dynamism of the technology environment and relative slowness of the policy response. It is not realistic to expect expert knowledge of technology from the policy-makers and an expert knowledge of policy from the technologists. We hope that the ontology proposed here can provide both philosophy and tools for defining a broadly applicable richer shared context that helps multi-stakeholder efforts to agree on the principles and provide operational context for norms.

The absence of mechanisms to transition more objectively from principles to norms hinders the development of common ground in complex and multidisciplinary fields, like cyber security. As an example, support for privacy is a shared principle in most cyber security strategies, but the nature of technical standards, norms, and best practices that are necessary in different technology contexts and the constraints imposed by technologies are not clear to the policy-makers, leading to imperfect regulations that are difficult to harmonise internationally. In other words, recognition of the essential character of privacy in connection with cyber security is not actionable without a predictable linkage to best practices (norms

6 Definition from Merriam-Webster, 'Principle,' http://www.merriam-webster.com/dictionary/principle.

7 'WSC Encryption Principles' (World Semiconductor Council, Lisbon, 23 May 2013), http://www.semiconductors.org/clientuploads/Trade%20and%20IP/May%202013%20WSC%20-%20WSC%20Encryption%20Principles-%20FINAL.pdf.

and standards), such as data anonymisation techniques or obfuscation of unique identifiers. In a different example, understanding of technology constraints, such as the impossibility of complete anonymity in today's computing environment, is necessary in order to create regulations and policies that are effective, such as guidelines for data protection. The introduction of a scientific reasoning process based on ontology that links policy principles and technical best practices would improve regulatory design and extend opportunities for self-regulation. Predictability would also increase trust in industry norms and best practices through the recognition of their connection to generally accepted principles in situations ranging from policy implementation to support for self-regulation.

The level of complexity of multi-disciplinary issues in cyber security also requires decision and dialogue support tools, and an ontology linking principles and norms can provide a foundation for such a mechanism.

1.4 Ontology as a Consensus-Building Tool

Ontology in computer science can be defined as 'a formal naming and definition of the types, properties, and interrelationships of the entities that really or fundamentally exist for a particular domain of discourse'.[8] Ontology permits us to highlight connections and relationships between terms, identify constraints, and to reason about a topic. Ontologies are commonly used in a variety of settings in cyber security, such as creating threat and vulnerability models for innovative fields.

Ontologies enable a structured organisation of knowledge and creation of a multifaceted context with reasoning capabilities. The complexity of the field of cyber security and the need to formulate relatively simple technical norms and best practices that are connected to general policy principles point to ontology as the tool of choice to capture relationships between concepts, principles, and their attributes and to enable robust modelling of constraints and complex situations.

While ontologies have been used in a number of fields, from e-commerce to enterprise systems, they have not yet been employed as a 'dialogue support' mechanism for multi-stakeholder initiatives in complex fields. For examples of ontologies used in knowledge engineering of diverse domains, repositories such as the Protégé Ontology Library[9] are recommended. Ontologies for cyberspace have also been created by, for example, Kopsell.[10] The introduction of a well-designed ontology could help the participants to create a framework for reasoning about cyber security norms in connection to shared principles, and to understand the mutual connections of the best practices, thus improving the efficiency of outcomes. The benefits will be significant for policy-makers and policy theorists, allowing them to improve their understanding of the complex technology space, and for industry, to support design and positioning of norms and best practices in a correct policy context.

8 See, for example, Wikipedia, 'Ontology (Information Science)', https://en.wikipedia.org/wiki/Ontology_(information_science).
9 Protégé Ontology Library, 'OWL Ontologies,' http://protegewiki.stanford.edu/wiki/Protege_Ontology_Library.
10 David R. Koepsell, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property*, (Peru, Illinois: Open Court Publishing, 2000).

Although we do not propose a concrete design for a 'multi-stakeholder dialogue support' ontology in this paper, we can identify foundations, upon which it can be built:

- *High level policy principles (top layer)* can be derived from commonly accepted key concepts identified by earlier efforts. This chapter is primarily focusing on this area.
- *Technology characteristics* can be established based on the accepted attributes of the technology environment and input from various experimental frameworks developed to analyse it.
- *Norms, standards and best practices* can be developed by the communities of experts and incorporated into the ontology.

The resulting ontology can arm multi-disciplinary initiatives with the ability to conduct in-depth conversations that rely on consistent background knowledge and do not over-simplify key issues, leading to better results. As an example, the Public Initiative on Cyber-Physical Systems (CPS) convened by NIST[11] proposed a risk-based framework for CPS that links risk domains of privacy, security, safety, resilience, and reliability in one integrated model. The insights resulting from this work can inform regulation and standardisation for the Internet of Things (IoT). The integrated risk model represents a set of general principles that can be used to analyse risk for the IoT. The reference framework produced by the same public working group extracts concrete elements that can make future IoT systems trustworthy. An ontology can link the high-level risk principles and concrete technical norms in this and similar initiatives, in order to permit technologists and regulators to jointly reason about optimal technology environments and the policy approaches that govern them.

Although a consistent shared context has not yet been generally adopted, even at the level of principles, some fundamental concepts have been defined as part of a number of industry- or government-led efforts. Incorporation of these elements of shared vision could speed up the creation of the body of knowledge to support consensus-building on major issues in cyber security. The section below describes these common elements as a potential foundation of a future shared context in an ontology to be used in multi-stakeholder initiatives. We start the discussion with the analysis of the most pertinent characteristics of the technology environment since they provide additional linkage between high level principles and norms.

11 Cyber-Physical Systems Public Working Group, http://www.cpspwg.org/.

2. Technology Environment

Today's dynamic technology environment supports seamless functioning of all societies around the globe. This section attempts to extract key characteristics of the technology environment that are also pertinent to policy-making in cyber security. We describe key characteristics that have been commonly recognised and that are broadly applicable. Broad categorisation of these attributes is illustrated in Table 2 below, and they form a foundation for technology principles to be used in the ontology we are describing.

Table 2. Key characteristics of the technology space by broad category.

Category	Attribute
Technology	Universal Connectivity
	Complexity and dynamic nature
	Influence on the physical environment
	Shared nature of infrastructure
Societal	Global and universal use of cyberspace
	Broad economic impact of cyberspace

2.1 Ubiquitous Connectivity and Interoperability

The modern computing environment is characterised by ubiquitous connectivity and interoperability between heterogeneous networks and diverse systems and devices. The numbers of connected devices cannot be estimated with great precision, but is extremely large. EMC Corporation estimates over 7 billion people will use 30 billion Internet-connected devices by 2020,[12] whereas Cisco and DHL predict a higher number – 50 billion connected devices by the same date.[13] Disparate computing and network domains of fifteen years ago have merged into an interconnected space that supports multiple models of use, connectivity, and access via shared infrastructure. The diversity of connected devices is enormous, including everything from data centres and full PC platforms to tablets, industrial control systems, disposable sensors and RFID tags, and it is matched by the diversity of the networks. Ubiquitous connectivity is beneficial for the users of the technologies and for the economy, leading to new efficiencies and increased productivity, and providing a platform for widespread innovation. The challenges created by this environment are well known. Universal connectivity and interoperability complicate the analysis of threats and vulnerabilities, lead to uneven levels of protection in interconnected systems and elements of infrastructure, and, in many cases, can increase attack surfaces.

Ubiquitous connectivity and broad interoperability support movements of data

12 EMC^2, *New EMC Innovations Redefine IT Performance and Efficiency*, 4 May 2015, http://www.emc.com/about/news/press/2015/20150504-01.htm.

13 Cisco, 'Internet of Things (IoT),' http://www.cisco.com/web/solutions/trends/iot/portfolio.html.

over diverse networks and are important for numerous areas of policy-making, including standards policies, network and information security regulations, and data protection. Policy developments that hinder the open nature of the Internet, such as data localisation or reliance on indigenous standards, can become obstacles to global interoperability and inhibit the role of cyberspace as a powerful engine of economic growth.

2.2 Intrinsic Complexity and Dynamism of the Technology Environment

Interoperable frameworks that form the foundation of the modern technology environment are likely to contain unknown vulnerabilities due to the effects of composition of diverse security models.

We have not yet developed mechanisms to analyse the composite picture of infrastructure that is today's reality. Complexity is obvious in the multi-domain processes typical of today, as there are a number of technical domains employed to achieve one operation. Although the process is designed to reach one operational goal, their security capabilities are different at different stages of the process. Defining 'trust evidence' for this environment has proved very challenging.[14]

With no objective approaches to estimating the security of complex systems under operational conditions and no standards to apply to diverse environments where they operate, it is difficult to comprehend the consequences of system level or environmental changes. This complexity and ambiguity also applies to data and data protection, making it necessary to re-think a number of fundamental concepts such as anonymity and data interoperability.

Complexity of the computing environment is the result of the aggregation of various frameworks and underlying security and privacy models that were designed in isolation. The impact of complexity needs to be well understood in order to correctly inform the development of effective cyber policies. Policy-makers frequently examine cyber security concerns at a simplified level, making generalisations that become disconnected from the evolving capabilities of the complex technology space. These policies need to be technology-neutral,[15] but also aware of the key characteristics of the technology space in order to incorporate the crucial relationships between norms and best practices in cyber security.

2.3 Intermingling of Cyber and Physical Components

Another important characteristic of cyberspace is the connection between cyber and physical environments, as exemplified in Cyber-Physical Systems (CPS), systems of systems that have computing components, communication capabilities, and

14 Claire Vishik, Anand Rajan, Chris Ramming, David Grawrock, and Jesse Walker, 'Defining trust evidence: research directions,' *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11)*, Frederick T. Sheldon, Robert Abercrombie, and Axel Krings, eds. (ACM: New York).

15 Technological Neutrality is 'the freedom of individuals and organizations to choose the most appropriate and suitable technology to their needs and requirements for development, acquisition, use or commercialisation, without dependencies on knowledge involved as information or data': Wikia, 'Technology Neutrality,' http://itlaw.wikia.com/wiki/Technology_neutrality.

physical subsystems.[16] CPS, now ubiquitous, requires more complex and integrated security and risk models. For CPS, the traditionally separated domains of safety, resilience, reliability, security, and privacy, are intertwined.[17] Separate assessment of these domains is insufficient to address the risks, because requirements optimised for one domain can be detrimental to the composite risk picture of a system or an area of infrastructure. Characteristics of CPS such as the presence of a physical subsystem and real-time controls may demand a departure from traditional views on security or privacy requirements and instead put an emphasis on safety and reliability, such as when developing risk models for nuclear power station management, where privacy concerns are minimal while safety and reliability requirements are crucial.

Stuxnet is an example of an attack carried through cyber-physical environments[18] that illustrates the need to analyse the requirements for all relevant risk domains using an integrated process. Only collaboration between multidisciplinary policy and technology teams can help address these risks. Tools supporting aggregation of different fields, such as the proposed ontology, can help in developing complex norms that span several risk domains, like privacy, cyber security, safety, and reliability.

2.4 Shared Global Infrastructure Based on Open Standards

The benefits of the shared global infrastructure and open standards are clear to all. We can use the same devices, applications, networks, and processes in France and Japan, China and Egypt; for the most part, technology now speaks a common language.

The consensus on the importance of the global shared infrastructure and open standards predates the commercial Internet, but concerns about its dependability emerged early in the Internet history and crystallised into a separate area of research in the mid-1990s.[19] Strong focus on the protection of critical infrastructure has led some researchers such as Dunn Cavelty to assert that 'militarisation of cyber security' was under way.[20]

The infrastructure is shared among the different users of cyberspace from education to transportation and energy, and by different geographic regions underlying the functionality of generic systems and processes. Uneven availability of expertise and resources has resulted in varying levels of cyber security and privacy protections in the infrastructure, stressing the need for policy-makers and technologists to continue to focus on capacity-building in cyber security.

16 See for example definitions at the Cyber-Physical Systems Public Working Group.

17 See deliverables of the NIST from Cyber-Physical Systems Public Working Group.

18 [Stuxnet] 'was a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant. … The key compromise was that Stuxnet placed itself in a critical path where it could not only disrupt the plant process, but also disrupt/manipulate the information flow to the system operator. In this particular instance of Stuxnet, it caused the fast-spinning centrifuges to tear themselves apart, while fabricating monitoring signals to the human operators at the plant to indicate processes were functioning normally.': David Kushner, 'The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program,' *IEEE Spectrum. IEEE*, February 26, 2013, 49-53. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet#.

19 Jeffrey Hunker, 'Policy Challenges in Building Dependability in Global Infrastructures.'

20 Myriam Dunn Cavelty, 'The Militarisation of Cyber Security as a Source of Global Tension,' in *Strategic Trends* 2012, ed. Daniel Möckli (Zurich: Center for Security Studies, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2007043.

2.5 Global Use of Cyberspace and Its Significant Impact on the Economy

Around 40% of the world's population used the Internet in 2014.[21] Twenty years ago, in 1995, the level of connectivity stood at 1% of the population. The number of Internet users grew at 7.9% in 2014, more than seven times faster than the population growth of 1.14%. Some 78% of the populations of developed countries and 31% of those of the developing world were connected in 2014.[22] With such a large population of users, cyberspace-dependent processes permeate the fabric of everyday life. The global nature and scope of cyberspace require strong understanding of the complex underlying technologies and patterns of use as well as policy frameworks enabling cyberspace use. Norms and best practices created in this context need to be actionable and broadly applicable.

The ICT sector has a significant impact on the global economy. By 2010, it represented 6% of global GDP and accounted for 20% of employment in OECD countries.[23] The sector is responsible for increasing productivity and improving efficiency in other sectors, and its impact on all aspects of everyday life and commerce is enormous. Although the development of the technology is rapid, the process of building a unified economic theory for cyber security and providing recommendation on optimal economic models to achieve improved security coverage has been slow.[24]

The digital economy magnifies the efficiencies achieved by monetary economies and creates economies of scale and scope via intermediation and aggregation of resources. Novel use models emerge and quickly become mainstream, providing a constant source of innovation and alleviating information asymmetry, as illustrated by Akelof's model.[25] Despite the rapid pace of change, there is limited theoretical work to address key economic issues, such as design of viable economic incentives for the development of secure infrastructure.[26] Slow development of the economic theory for cyber security is an inhibitor for the design, implementation, and harmonisation of broadly applicable policies, metrics and the model necessary for building and evaluating cyber security norms.

21 Statistics from Internet Live Stats, 'Internet Users,' http://www.internetlivestats.com/internet-users/.

22 International Telecommunications Union (ITU) estimate: Wikipedia, 'Global Internet Usage,' https://en.wikipedia.org/wiki/Global_Internet_usage.

23 'Moving Forward Together: Recommended Industry.'

24 Johannes M. Bauer and Michel J. G. Van Eeten, 'Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options,' *Telecommunications Policy* 33 (2009): 706-719; and Eric Luiijf, et al, 'Ten National Cyber Security Strategies: A Comparison,' in *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers*, ed. Sandro Bologna et al. (Springer-Verlag Berlin Heidelberg, 2013), 1-17.

25 George A. Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism,' The Quarterly Journal of Economics 84 (1970): 488-500.

26 Claire Vishik, Frederick Sheldon and David Ott, 'Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment,' in *ISSE 2013 Securing Electronic Business Processes*, eds. Helmut Reimer, Norbert Pohlmann and Wolfgang Schneider (Springer Vieweg, 2013), 133-147.

3. Extracting High Level Concepts for the Ontology

Section 2 explored fundamental technology characteristics of cyberspace. The goal of section 3 is to extract high-level common elements from diverse sources that address both policy and technology aspects of cyberspace and that can be used to populate top levels of the proposed ontology. With no accepted framework in place for the co-development and analysis of technology and policy approaches for cyber security, we find useful input in related research, policy analysis, and industry papers. These common elements reflect shared interests and concerns among industry and government, and thus should form a foundation for an ontology supporting multi-disciplinary work on cyber security policy approaches and norms, by allowing industry to design best practices (technical and process norms) consistent with the accepted high level principles, and by enabling the policy community to understand the connection between the principles and best practices guiding their concrete implementation. It is not a comprehensive list of sources and key concepts, but it is representative, and the sources that we evaluated produced overlapping sets of high-level concepts, suggesting shared views on many aspects in cyber security.

3.1 Theoretical Research Frameworks

A number of technology and policy frameworks have been proposed to enable or facilitate the examination of multidisciplinary subjects in security and privacy. A good example is Technology Dialectics,[27] a model developed by Professor Sweeney to mitigate conflicts between requirements of technology and context of use in society. The goal is to detect potential social and adoption issues early in the technology cycle and resolve them by creating tools to determine whether a technology is demonstrably appropriate for a certain society or context. Although the framework focuses on privacy, it can be used for broader analysis and easily applied to cyber security.

Similar single-domain technology and policy frameworks have been proposed by various researchers, including Golubchikov and Deda for the study of low-energy housing,[28] and Ananda, Pandy, and Punia for the analysis of the power sector in India.[29] The shared elements found in this work are summarised in Table 3 below.

27 Latanya Sweeney, 'Technology Dialectics: Constructing Provably Appropriate Technology,' *Data Privacy Lab* (2006), http://dataprivacylab.org/dataprivacy/projects/dialectics/index.html.

28 Oleg Golubchikov and Paola Deda, 'Governance, Technology, and Equity: An Integrated Policy Framework for Energy Efficient Housing,' *Energy Policy* 41 (2012): 733-741.

29 V. Ananda Kumar, Krishan K. Pandey and Devendra Kumar Punia, 'Cyber Security Threats in the Power Sector: Need for a Domain Specific Regulatory Framework in India,' *Energy Policy* 65 (2014): 126-133.

Table 3. Relevant components of technology/policy frameworks.

Category	Key concepts
Technology	Broad applicability
	Rapid innovation
	Shared infrastructure and context requirements
	Diverse operational models
Societal	Evolving use models and context
	Complex requirements for adoption
	Economic considerations
	Connection to fundamental rights (e.g., privacy)
Approach	Actionable (rather than observational)
	Capable of evolution
	Provably effective

The characteristics found in the technology and policy frameworks that we examined are consistent with those we discussed in section 2. These concepts are useful to inform ontology development, and they point to ontologies as support tools linking technology and societal issues. Similar frameworks are frequently employed to support technology development processes in industry.

3.2 Cyber Security Strategies

Another source of shared high-level concepts is found in cyber security strategies formulated by different countries. The OECD's report, *Cyber Security Policy-Making at a Turning Point: Analysing a New Generation of National Cyber Security Strategies for the Internet Economy and Non-governmental Perspectives on a New Generation of National Cyber Security Strategies: Contributions from BIAC, CSISAC and ITAC*, reveals that cyber security strategies developed by different nations share a number of common elements. Shared approaches include the stated need for enhanced internal operational coordination; reliance on private-public partnerships, interest in improved international coordination, the need to protect fundamental values in cyberspace,[30] as well as reliance on flexible policies for cyber security, supporting the economic development associated with the ICT sector, and engagement in multi-stakeholder dialogue. Other researchers such as Kshetri and Murugesan, who compared the US and EU cyber security strategies,[31] and Luiijf, who examined ten cyber security strategies, highlight similar elements of shared cyber security vision. Common elements of cyber security strategies are summarised in Table 4.[32]

Private ownership and operation of critical infrastructure mean that all the stakeholders (government, academia, industry, and non-profits) need to collaborate

30 'Cybersecurity Policy-Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy and Non-Governmental Perspectives on a New Generation of National Cybersecurity Strategies: Contributions from BIAC, CSISAC and ITAC' (Organization for Economic Co-operation and Development, 16 November 2012), 9, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

31 Nir Kshetri and San Murugesan, 'EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers,' *Computer* 46 (2013): 84-88.

32 Luiijf, et al, 'Ten National Cyber Security Strategies: A Comparison,' 1-17.

on cyber security issues in order to mitigate cyber threats and enhance resiliency and security while maintaining the interoperability and open Internet.[33] But diverse stakeholders cannot acquire expertise in all the relevant topics. Arming multi-stakeholder initiatives with tools such as a comprehensive ontology, in addition to the typical high level deliverables of multi-stakeholder dialogue, e.g., position papers, can bring more efficiency to the process, allowing industry to elucidate the viability of norms and best practices in a broader context that is easier to understand.

Table 4. Common elements shared by cyber security strategies based on OECD[34] report and other analyses.

Type of Elements	Common Elements	Description
Societal/economic	Economic impact	Quantification of economic benefits of cyber security into the strategy
Organisational/policy	Enhanced government cooperation	Better policy level and operational coordination among multiple agencies
	Public-private cooperation	Engagement of all stakeholders (government, industry, non-profits) in policy and solutions development
	International cooperation	Collaboration with other countries on a range of cyber security issues
	Division of responsibility among various government organisations and sovereignty	Operational role of agencies responsible for national security
	Support for fundamental values	Recognition of fundamental values, such as freedom of expression, privacy protection and the free flow of information as essential
Technology-related	Innovation	Preservation of open Internet as a platform for innovation and economic growth
	Comprehensive coverage	Strategies address the full range of ICT components

3.3 Industry-Led Initiatives

Another source of high-level concepts is furnished by documents created by industry and industry associations. The white paper prepared by five industry associations for Cyber Seoul 2013 provides useful categorisation of areas of focus: economic considerations, social and cultural benefits, cyber security proper, international security, cyber crime, and capacity-building as summarised in Table 5.[35] The paper, which is based on a number of earlier sources, indicates high-level areas which are important for industry and to which more specific norms need to be anchored.

33 'Cybersecurity Policy-Making at a Turning Point,' 10-15.

34 Eric Luiijf, Kim Besseling and Patrick de Graaf, 'Nineteen National Cyber Security Strategies,' *International Journal of Critical Infrastructure Protection* 9 (2013): 7-26; 'An Evaluation Framework for National Cyber Security Strategies' (European Union Agency for Network and Information Security, 11 November 2014), 30-31, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies; 'Cybersecurity Policy-Making at a Turning Point,' 9, 24-52.

35 'Moving Forward Together: Recommended Industry.'

Table 5. High-level categories from Seoul industry paper (2013).

Type of Elements	Key Area	Description
Economic	Economic growth and development	Economic growth is the key contribution of the ICT sector
Policy (legal, organisational)	Development of legal frameworks	Criminal statutes to clarify and enhance law enforcement's ability to prosecute bad actors, to combat cyber crime and enhance international cooperation are available
	International cooperation	Cooperation to advance social, economic, and cultural goals, given cyberspace offers a unique global commons
	Capacity-building	Cooperation to develop additional capabilities in legal, policy, and technology areas
	Response to cyber threats	Cooperation to prevent, detect, and respond to cyber security threats.
	Response to cyber crimes	Work to deter cyber threats, implement tools to identify criminal activities, and carry out coordinated action
Societal	Societal and cultural benefits	Increased access to education, influence on the political process, and support for human rights

The paper illustrates a significant level of convergence on high-level principles between the industry and governments that participated in the Seoul Conference on Cyberspace 2013, based, for example, on the similarities between these approaches and the approaches reflected in cyber security strategies produced by various governments, as described above. An ontology linking these key concepts and more concrete best practices could enable diverse communities to collaborate in greater depth and develop more actionable norms and policies.

3.4 Global Digital Infrastructure Work

Industry, academia and government have developed a number of position papers that provide insights into novel policy approaches that support key trends in technology evolution. Among these documents, Intel's *Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy*[36] explains the foundational nature and importance of Global Digital Infrastructure (GDI) and the need to develop policies that support GDI-based innovation and preserve the users' trust in the digital economy. These policies should support the environment that ensured the success of GDI; openness, interoperability, and economic growth potential and should be technology neutral, based on open standards, fostering international cooperation and strong accountability. The underlying concept is 'the triangle of trust' – a collaboration of industry, government, and NGOs on broadly applicable policy principles, including self-regulation and consumer awareness and education.

Other recent research efforts have studied other aspects of GDI, describing GDI evolution and associated metrics.[37] Max Craglia (2015), editor of the joint project of

36 John Miller and David Hoffman, 'Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy,' *Intel Corporation* (2010), http://blogs.intel.com/wp-content/mt-content/com/policy/Global%20Digital%20Infrastructure%20Policy%20Merged.FINAL.PDF.

37 Ola Henfridsson and Bendik Bygstad, 'The Generative Mechanisms of Digital Infrastructure Evolution,' *MIS Quarterly,* 2013, (37: 3), 896-931.

the Chinese Academy of Sciences and the European Commission on Digital Earth 2020, stressed the importance of incorporating policy constraints when developing specific technologies, in order to avoid complications and speed up adoption, echoing the main thrust of the Technology Dialectics framework.

Table 6. GDI and GDI policy: principles.

Type	Broadly applicable principle	Description
Technology	Interoperability	Seamless interoperation among the components of infrastructure and ecosystem
	Openness	Free flow of data across borders and global access to and sharing of innovation
	Foundation in open standards	Support for innovation, collaboration, and openness without relying on particular technologies
	Dynamic nature and rapid evolution	Quick pace of innovation affecting technology and use models
Societal	Economic growth potential	Strong economic growth with cross-sectoral collaboration
Policy	Self-regulation	Self-imposed rules based on based practices and optimal technology outcomes
	Multi-stakeholder international cooperation	Cooperation across borders and sectors to promote continued innovations, economic growth and trust
	Accountability	Obligation/willingness to take responsibility for performance based on agreed-upon expectations

The high-level common elements and principles discussed in this section form an overlapping representative list drawing from diverse sources produced by industry, government, academia, and non-profits. These concepts and the relationships between them can be used to populate the top level of the ontology we are proposing to support multi-stakeholder work in cyber security.

4. Major Gaps That We Need to Address

In order to create a viable common context for the diverse stakeholders in cyber security, additional research, analysis, and industry assessment efforts are needed. Section 4 identifies some of the more important gaps that need to be addressed.

4.1 Scientific Foundations for Cyber Security

The last decade saw several efforts to move cyber security from a practical discipline to a more theoretical level; to develop a 'science of cyber security' that could provide a common foundation for the increasingly diverse range of cyber security topics. The Federation of American Scientists (FAS) described the issue as follows:

> 'The challenge in defining a science of cyber-security derives from the peculiar aspects of the field. The 'universe' of cyber-security is an artificially constructed environment that is only weakly tied to the physical universe. … Cyber-security requires understanding of computer science concepts, but also shares aspects of sciences such as epidemiology, economics, and clinical medicine; all these analogies are helpful in providing research directions.'[38]

The report concludes:

> 'There is a science of cyber-security. Because it is a science with adversaries, it uses, and will use, many different tools and methods. For the future, as far as can be discerned, there will be new attacks on old technologies, and new technologies that need to be defended.'[39]

Cyber security is a science with mature subfields, but lacking accepted definitions of fundamental concepts such as security composition, assurance, accountability, or trust. Strong and generally accepted scientific foundations for cyber security will be instrumental in developing approaches to policy design and norm development based on shared principles already defined by earlier efforts. We hope that an ontology that we are describing here can be instrumental in unifying definitions and methodologies in different areas of cyber security, in addition to linking technical norms with policy principles.

4.2 Standardisation Strategy, Process, and Policy

Open standards enable the foundation of today's digital infrastructure and are crucial for the seamless operation of cyberspace. Active work on the development of international standards is conducted in a variety of settings, from international (for example, ISO, IEC, and ITU)[40] and national standards bodies (ANSI, BSI, or DIN)[41] to industry standards consortia (IEEE or TCG)[42]. It is recognised that most general-purpose technology and governance standards and specifications have to address security and, in many cases, privacy in order to be viable. The inventory of potentially relevant standards existing today is enormous. There are solid internationally recognised policy mechanisms set up to support the use of open standards, including agreement within the World Trade Organization. Standards are necessary to enable the foundations of the dynamic and open cyberspace.

However, in the area of cyber security, there is a lingering perception that, in order to strengthen national security, open international standards should not be

38 Jason, The MITRE Corporation, *Science of Cyber-Security*, JSR-10-102 (19 November 2010), 1, http://fas.org/irp/agency/dod/jason/cyber.pdf.

39 Ibid, 77.

40 IEC (International Electro-technical Commission), ISO (International Organization for Standardisation), ITU (International Telecommunication Union).

41 *American National Standards Institute (ANSI),* British Standards Institution (BSI), Deutsches Institut für Normung e.V. (German Institute for Standardisation) (DIN).

42 The Institute of Electrical and Electronics Engineers (IEEE), Trusted Computing Group (TCG).

used, even in general-purpose technology environments, and that local or regional standards provide greater security because knowledge about them is more limited. These misconceptions have been disproved by extensive research, and continued development of indigenous standards represents a potential threat to the global nature of the Internet and may exclude some constituencies from using the latest most robust security technologies. Among the areas in standardisation that require further development, the following gaps stand out:

- The dearth of global cyber security standards strategy that can address current priorities, e.g., in the infrastructure area;
- The absence of faster and more efficient processes and greater directional flexibility in standardisation, to match the dynamic nature of today's technology environments;
- A lack of methodologies to address harmonisation of standards policy in different countries and regions; and
- No mechanisms to incorporate regional requirements without jeopardising the global nature of the cyber security standards.

The gaps in the standardisation approaches stem from structural issues, which have led to fragmentation of efforts to develop standards. Many organisations, regionally and internationally, have engaged in developing standards for the same or similar spaces. Examples include international (ISO/IEC) and Chinese standards for a Trusted Platform Module; differing regional approaches to Internet governance and numerous overlapping efforts focusing on IoT standardisation in such organisations as IEEE, ISO/IEC, or ETSI. An ontology that is proposed here can have a unifying influence on both technical and governance standards, allowing the stakeholders to address cross-cutting issues in standardisation for cyber security instead of treating these issues in isolation for each context.

4.3 Absence of a Common Vocabulary and Reasoning Framework

The dynamic evolution of cyberspace and its global nature require multidisciplinary study in a process that can support ideation, harmonisation, deployment, adoption, and maintenance of cyber security technologies and policies in a multi-stakeholder setting.

Policy and technology communities, government, and industry use different paradigms to address shared concerns. Cultural gaps can result from different backgrounds, traditions, and different operational contexts. National security communities, energy and finance sectors, high-tech industry, and other key players use different frameworks to address similar security issues. While policy researchers and policy-makers look at the cyber security landscape from a strategic perspective based on general philosophy of the subject, engineers tend to focus on technology considerations and are frequently unaware of the impact national or international regulations and geopolitical concerns could have on their work. Technologists have

different work cycles and objectives, and use different language to policy researchers and policy-makers to describe similar issues.

In order to overcome cultural and knowledge gaps between policy researchers, regulators and the technical community, a common framework and common vocabulary need to be developed. The lack of this shared context is a major stumbling block leading to the fragmentation of the work of different communities of research and practice. An ontology can furnish reasoning and analysis capability in addition to a common vocabulary, providing a mechanism to overcome cultural differences.

5. Towards a Shared Context: Connecting Principles and Norms

Analysis of literature on different aspects of cyber security furnished us with a list of multi-disciplinary fundamental concepts and principles for the integrated analysis of cyber security issues. These elements could serve as a foundation for an ontology to support more efficient multi-stakeholder dialogues in policy, technology, standardisation, and other areas, and for studying cyber security as a multi-disciplinary scientific subject, incorporating societal, technology, and policy contexts.

The lack of a provable ontology-based connection between high level principles and recommendations, technical feasibility of proposals, pace of innovation, efficiency, and enforceability plays a role in complicating negotiations on complex issues, such as the new Data Protection and Network and Information Security regulations in the European Union. The complexity of the issues requires unrealistic knowledge of the broader context from all the participants. Availability of a broadly applicable 'dialogue ontology' would allow industry to demonstrate how technical norms and best practices support high-level principles and recommendations. Such tools would also help illustrate technology constraints in proposed approaches and find remedies to eliminate contradictions. An ontology would help reduce ambiguity by establishing definitions and relationships between concepts and permitting the stakeholders to reason about consequences of the proposed regulations or the requirements of the current technology solutions and processes, such as international data flows. Most importantly, an ontology linking high-level principles and concrete technical or process norms and best practices would be instrumental in outlining a clearer direction towards the implementation of accepted policy proposals. It would permit the participants to speak the same language, to use the same decision support tools, and to define problems and solutions in the same or similar terms without acquiring comprehensive knowledge of issues.

The use of key concepts as the highest level of the ontology can speed up its development and shorten the discussions associated with the structure of the ontology. An ontology will help avoid over-simplification of cyber security principles and provide a framework to incorporate norms and best practices, linked with the principles in a predictable fashion.

In order to create the common context for in-depth reasoning in support multi-stakeholder discussions, we need to link abstract ideas and concrete actionable concepts, account for dynamisms and rapid evolution of cyberspace, address governments' concerns and users' requirements, and understand the implications created by the technology space. We need to be able to make sense of regional differences and complex patterns of adoption, understand limitations of current approaches, and be able to model radically new solutions.

From the technology point of view, cyberspace is rooted in shared global digital infrastructure (GDI) and includes a variety of technology domains that can form a large number of dynamic contexts. Among these contexts, we can identify smart grid, connected transportation and energy, online education, social networks, organisational and government environment, as well as broader foundations of these contexts, such as 'cloud' or the 'Internet of things'. The environment comprises multiple interconnected technology components such as networks, devices, and data, and also possesses user interfaces and, in some case, physical subsystems.

The technology space has a number of important characteristics that have strong impact on the development of policies and technical norms. They include intrinsic complexity, interoperability, ubiquitous connectivity, and intermingling of diverse contexts, such as cyber and physical. These characteristics need to be taken into consideration in every policy and technology strategy initiative. Over-simplification of cyberspace, while helpful in some contexts, is a poor initial premise for a policy discussion and limits the necessary assessment of constraints and interdependencies impacting the effectiveness of an approach, a legal framework, or a regulation.

The technology space brings significant societal benefits, but its continued success depends on the acceptance of innovation by the society. It has been an economic driver and engine of innovation since its emergence, and has acquired an enormous user base, with 40% of the global population connected, providing access to education, information, and entertainment, supporting consumer and work environments, and underlying every element of critical infrastructure. The consequences of even a small failure of this system of systems are hard to quantify.

The technology environment is based on fundamental characteristics linking the technology environment with the policy space and providing a foundation for the development of industry norms and best practices for cyberspace. Because of the complexity of the environment, cyber security risks are multi-faceted, comprising the adjacent domains of security, privacy, safety, reliability, and resilience. These risk domains can be addressed through private-public collaboration, international cooperation, national coordination, and multi-stakeholder efforts, the key

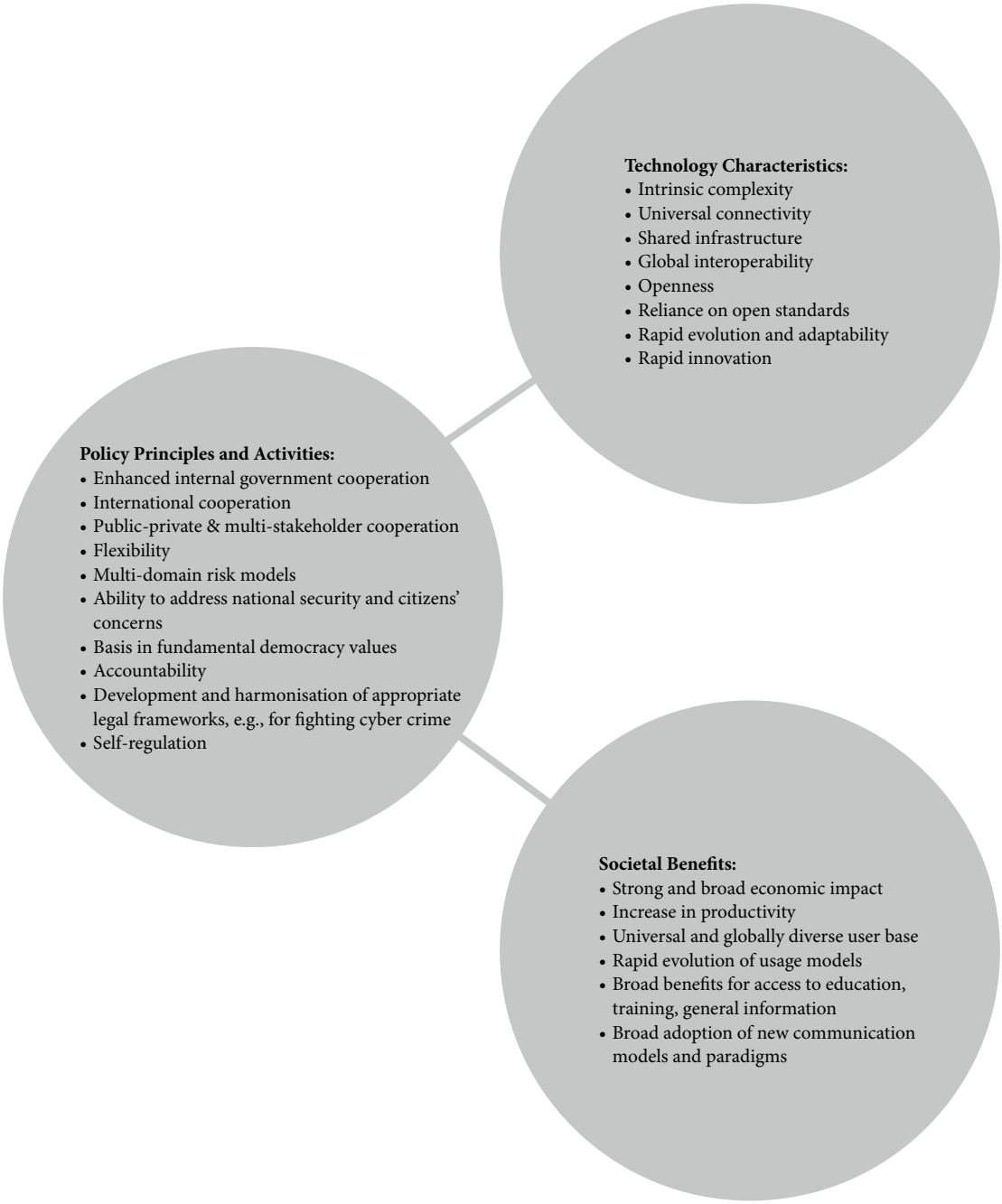

Figure 1. Consolidated graphic of key concepts and principles – high level of the proposed ontology.

approaches shared by cyber security strategies of multiple countries such as Information Sharing and Analysis Centre (ISAC) efforts.

Policies necessary to support the rapid development of the technology space and the societal benefits it fosters have to be based on the integrated characteristics of the cyber environments, and the attributes and principles upon which these characteristics are built. They need to include a well-defined connection between technology norms and best practices, and high-level policy principles. Such a connection is necessary in order to define policies and regulations in a way that makes them compatible with the technology environment. The meaning of key principles such as support for privacy or transparency needs to be reinforced by the link with technical and process best practices that is necessary to operationalise these concepts. A rich ontology linking principles with norms and best practices can help in maintaining a unified, but actionable model of cyberspace and in forming objective links between the layer of principles and the layer of norms and best practices.

6. Conclusions

The international harmonisation of cyber security strategies and visions has not yet been achieved, but the analysis of diverse literature on cyber security and cyberspace shows a degree of coherence for high-level concepts and displays evidence of commonality in concepts, principles, and attributes describing various aspects of policy, technology space, and societal impacts of cyberspace. This commonality provides a reservoir of fundamental concepts and principles that can help industry, government, academia, and others to develop an in-depth view of cyberspace.

These common concepts and principles covering technology, policy, and societal issues can serve as a foundation of a shared approach to cyber security devised as an ontology. The ontology could connect high-level principles developed by policy efforts and best practices designed by industry experts. It could be instrumental in creating a common context to support multi-stakeholder interactions, could help to model and predict the rapid pace of chance in cyberspace and could enable a multi-disciplinary scientific view of cyber security.

Although we did not build a prototype ontology to support the ontology proposal in this paper, such an ontology could be quickly developed based on the top-level concepts we proposed and with the use of common ontology tools such as Protégé[43] and based on the methodology described here. The development of such an ontology is a worthy topic for a multi-disciplinary community effort.

43 Protégé, http://protege.stanford.edu/.

Industry has developed a set of best practices and norms in cyber security, such as technology and governance standards, best practices for privacy and data protection, and secure technology development. They are based on high-level principles evolved by the global community. However, the connection between norms and principles remains abstract, hindering mutual understanding in multi-stakeholder initiatives and harmonisation efforts. We believe that an ontology permitting diverse stakeholders to reason about the complex environment can provide tools leading to greater mutual understanding and, as a result, to greater progress in cyber security initiatives.