

# Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity

Kharlamov, Alexander; Pogrebna, Ganna

DOI:

[10.1111/rego.12281](https://doi.org/10.1111/rego.12281)

License:

Creative Commons: Attribution (CC BY)

*Document Version*

Publisher's PDF, also known as Version of record

*Citation for published version (Harvard):*

Kharlamov, A & Pogrebna, G 2019, 'Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity', *Regulation & Governance*.  
<https://doi.org/10.1111/rego.12281>

[Link to publication on Research at Birmingham portal](#)

## General rights

Unless a licence is specified above, all rights (including copyright and moral rights) in this document are retained by the authors and/or the copyright holders. The express permission of the copyright holder must be obtained for any use of this material other than for purposes permitted by law.

- Users may freely distribute the URL that is used to identify this publication.
- Users may download and/or print one copy of the publication from the University of Birmingham research portal for the purpose of private study or non-commercial research.
- User may use extracts from the document in line with the concept of 'fair dealing' under the Copyright, Designs and Patents Act 1988 (?)
- Users may not further distribute the material nor use it for the purposes of commercial gain.

Where a licence is displayed above, please note the terms and conditions of the licence govern your use of this document.

When citing, please reference the published version.


## Take down policy

While the University of Birmingham exercises care and attention in making items available there are rare occasions when an item has been uploaded in error or has been deemed to be commercially or otherwise sensitive.

If you believe that this is the case for this document, please contact [UBIRA@lists.bham.ac.uk](mailto:UBIRA@lists.bham.ac.uk) providing details and we will remove access to the work immediately and investigate.



# Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity<sup>†</sup>

Alexander Kharlamov 

University of the West of England, Frenchay Campus, Bristol, UK

Ganna Pogrebna 

The Alan Turing Institute, London, UK

Department of Economics, Birmingham Business School, University of Birmingham, Birmingham, UK

## Abstract

This article develops a new framework linking cross-cultural human values, regulation, and governance in the area of cybersecurity. Cyber space is currently transitioning from a *laissez-faire* into a regulated area. Yet, there is a significant heterogeneity in terms of the strength of commitment in different states to regulation and governance of digital spaces. Therefore, it is important to explore why this heterogeneity exists. This article proposes that heterogeneity in the commitment to regulation and governance of cyber space between different nations stems from the fundamental cross-cultural differences in human values between countries. Using an example of cybersecurity, we show how the cultural value orientations theory maps onto national commitments to regulate and govern cybersecurity issues. We construct a theoretical framework linking human values with cybersecurity regulation and confirm the existence of this link empirically using the data from the international Schwartz Value Survey and the Global Cybersecurity Index.

**Keywords:** cybersecurity, governance, human values, regulation.

## 1. Introduction

We are living in the era when the Internet is being transitioned from completely free, *laissez-faire* area into a place, which is becoming more and more regulated by law. This, in turn, has significant implications for a wide variety of IT services, for the management of IT resources, as well as for the economics of IT, greatly affecting all facets of the digital life for the entire global community. When we consider the Internet regulation, we observe considerable heterogeneity across different countries around the globe ranging from nations, where regulation is pronounced and consistent, to nations, where little or almost no regulation is applied.<sup>1</sup> Under these circumstances, it is important to establish why we observe such a heterogeneity in the Internet regulation. For the purposes of this study, we will particularly concentrate on regulation and governance of cybersecurity.

Many of the national regulations which concern cybersecurity are designed in a similar fashion to regulations relating to public safety and security (e.g. Clark *et al.* 2014). Specifically, public safety matters are usually regulated based on the outcomes of quantified risk assessment exercises (such as risk cost–benefit analysis or RCBA) where potential hazards from activities or events are evaluated against probabilities of these hazards (e.g. Wolff

Correspondence: Ganna Pogrebna, The Alan Turing Institute, 96 Euston Road, Kings Cross, London NW1 2DB and the Department of Economics, Birmingham Business School, University of Birmingham, JG Smith Building, Birmingham B15 2TT, UK. Email: g.pogrebna@bham.ac.uk

<sup>†</sup>We are grateful to the editor and three anonymous referees for many helpful comments and suggestions which allowed us to significantly improve this article. Ganna Pogrebna acknowledges financial support from the grant UK Research and Innovation EPSRC grant EP/P011896/2. Ganna Pogrebna also thanks Economic and Social Research Council and the Alan Turing Institute for the fellowship support (grant ES/R007926/1). We also thank Professor Shalom H. Schwartz as well as the International Telecommunications Union (especially to Maxim Kushtuev) who provided datasets used in this article.

Accepted for publication 29 August 2019.

2006). Several papers in information systems as well as in philosophy argue that such “context-free” RCBAAs are often inadequate to approach situations involving unknown or unanticipated dangers and hazards much like those we face in cyberspace (see e.g. Wolff 2006 ; Hillson & Murray-Webster 2012). Notably, Wolff (2006) recognizes that safety and security risk regulation often not only requires understanding of actual (objective) risk taking, but also necessitates the comprehension of how various risks are perceived. Furthermore, in many situations, the understanding of context in which security risk originates is extremely important (Wolff 2006).

Traditionally, it is implied that a system of regulations and regulatory mechanisms (at least to some extent) represents the system of values for a particular population (e.g. Feather 1994). For example, in his famous lecture, Chief Justice James Allsop argued that “Law, at its very foundation, is conceived and derived from values... These values find their expression not only in the formal law, but also in societal expectations, behaviour and actions...” (Allsop 2017, p. 1). The link between values and safety regulations has also long been established in the philosophical literature on public safety (e.g. Wolff 2002, 2006). Specifically, Wolff (2006) argues that “safety has a price, in terms of impact on other things we want or value, and there are limits to what we are prepared to pay.” (Wolff 2006, p. 411). Yet, it is not clear whether human values, which are impacting on regulation and governance of physical and moral spaces, are also important in cyber spaces.

The purpose of this article is to address the following question: is the heterogeneity in cybersecurity regulation and governance rooted in fundamental difference in human values between different countries? We propose a new human values-based framework for understanding cybersecurity regulation and governance which has a theory of cultural value orientations (Schwartz 2006) at its core. Using this framework, we make a distinction between two types of nations: (i) nations with more competitive (individual-based) social value systems; and (ii) nations with more cooperative (collective-based) social value systems. We then formulate hypotheses about commitment to cybersecurity for nations of type (i); and type (ii) and test these hypotheses utilizing field data. Through these empirical tests, we establish a strong link between human values and the state commitment to regulation and governance of cybersecurity suggesting that regulatory systems and processes which help societies govern digital domains are rooted in their values and culture.

The remainder of this article is structured as follows. In Section 2, we present our theoretical framework, summarize our hypotheses, as well as describe our dataset. In Section 3, we conduct an empirical analysis using statistical tests and econometrics. Finally, Section 4 concludes.

## 2. Toward human values-based framework of cybersecurity preferences

### 2.1. Human values, attitudes, and regulation of cyberspace

Much literature in legal and social studies considers the link between human values and justice systems, regulation (especially, safety regulation), and governance in traditional (noncyber) domains (see, e.g., Feather 1994; Wolff 2006). Particularly, Wolff (2006) argues that “...the proper aims of safety regulation and the proper means of achieving these aims are moral issues” (Wolff 2006, p. 409). Yet, to date, the link between human values and cybersecurity regulation and governance has not received sufficient attention. Research, presented in this article, aims to address this gap in the existing literature.

Our contribution is rooted in combining three streams of research: (i) *literature on regulation and governance of security*; (ii) *literature on human values and their measures*; as well as; (iii) *literature on human values and security governance*. *Literature on regulation and governance of security* is a rapidly growing stream of research, which looks at the relationship between the state, governance in its traditional sense, and new ways of regulation (including social regulation) in relation to policing, security, and safety. Although this literature is vast, several papers are particularly relevant to our study. Specifically, Crawford (2006) provides a detailed overview of this research stream and argues that in the modern digital age, governance and regulation of security tend to be more and more engaged with and relate to human psychology, for example, through application of social engineering techniques by governments. Johnsten and Shearing (2003) as well as Shearing and Johnston (2013) argue that contemporary regulation and governance of security is more and more synchronized with human values and human psychology as “the state has been de-centred from the delivery and regulation of policing, and the trend is towards ‘community’ displacing ‘the social’ as the sign under which collective life is imagined and secured”(Loader & Walker 2004, p. 221).

*Literature on human values and their measures* is another stream of research, relevant to our study. Social sciences provide many definitions of human values. For example, Rokeach (1973) views values as beliefs of a higher level of abstraction than attitudes and preferences. An extended definition of human values is provided in Feather (1982) who defines them as

Organized summaries of experience that capture the focal, subtracted qualities of past encounters, that have a normative or oughtness quality about them, and that function as criteria or frameworks against which present experience can be tested... But they are not affectively neutral abstract structures. They are tied to our feelings and can function as general motives. (Feather 1982, p. 275).

Although some human values such as “rejection of unfairness;... insistence on essential quality; respect for integrity and dignity of the individual; and mercy” seem to “transcend cultural boundaries” (Allsop 2017, p. 1), several papers considered heterogeneity in human values across different nations and cultures. Particularly, Rokeach (1973) developed the Rokeach Value Survey (often referred to as RVS) which consisted of 18 terminal and 18 instrumental values ranked by respondents according to their relative importance to self. *Terminal* values represented generalized (ultimate) goals or outcomes such as equality, freedom, family security, and so forth; whereas *instrumental* values captured major modes of conduct such as honesty, love, responsibility, and so forth.

RVS was later extended and remapped by Schwartz (1992) who later developed the cultural value orientations theory (see Schwartz 2006). The new Schwartz Value Survey (often referred to as SVS), which formed the basis of the cultural value orientations theory, allowed respondents to rate 56 (in more recent samples, 57) values according to their importance as a “guiding principle” of a respondent’s life on a scale from  $-1$  to  $7$ , where the answer “opposed to my values” received score of  $-1$ ; “not important” received a score of  $0$ ; “important” received a score of  $3$ ; and “of supreme importance” received a score of  $7$ .<sup>2</sup> The initial version of SVS divided values into terminal and instrumental similarly to the RVS. The cultural value orientations theory partitioned values into six broad value dimensions: Embeddedness, Autonomy, Harmony, Mastery, Egalitarianism, and Hierarchy.

In the cultural value orientations theory, six value dimensions are polarized forming pairs of antithetical constructs. Specifically, although Harmony refers to the human desire to fit into the environment without trying to change it, Mastery depicts the human tendency to take control and direct the environment (Schwartz 2006). Although Egalitarianism refers to the human belief that people should be “moral equals who share basic interests as human beings” (Schwartz 2006, p. 140), Hierarchy “relies on hierarchical systems of ascribed roles to insure responsible, productive behavior” (Schwartz 2006, p. 141). Embeddedness implies that people are viewed as a part of some collective entity, and Autonomy represents a polar view where people are considered to be autonomous entities bounded by the society. Autonomy is also divided into two subdimensions: Intellectual and Affective Autonomy.<sup>3</sup> Intellectual Autonomy refers to people’s desire to follow their own ideas and creativity, and Affective Autonomy depicts the human goal to pursue personal gain in the form of satisfaction, excitement, and so forth. (Schwartz 2006).

We have chosen the Schwartz’s theory of cultural value orientations over other existing theories of human values because this theory has several important advantages over its competitors, for example, Hofstede’s five-dimensional theory (Hofstede 1980 and 2001) and Inglehart’s two-dimensional theory (Inglehart 1977 and 1990). First, Schwartz’s theory offers a more general approach to human values, which originates in psychological research, and, therefore, has a broad range of applications. In contrast, Hofstede’s theory looks primarily at work values and is mostly applicable to business and management applications, although Inglehart’s theory mostly concentrates on the effects of modernization and is rooted in materialism–postmaterialism literature stemming from political science and sociology. Second, unlike Hofstede’s and Inglehart’s theories, which primarily emerged from empirical observations and analysis (specifically, from factor analysis of collected data), Schwartz’s approach was first formulated theoretically and then validated empirically using large samples of observations from many different countries. Third, value constructs used by Schwartz have proven to be robust over the years as repeated measurements conducted between 1988 and 2018 showed that both absolute and relative measures of human values from different countries do not appear to change much despite socio-economic and political shifts (e.g. Schwartz *et al.* 2010 ; Schwartz & Sortheix 2018). Fourth, unlike other approaches, Schwartz’s theory uses only *abstract and basic values* relevant to all societies (e.g. social justice, creativity, etc.) irrespective of people’s political views or socio-economic status. To ensure this “universality” of values, Schwartz’s theory is based on a set of important features: “(1) [v]alues are beliefs...linked to affect; (2) [v]alues refer to desirable goals...; (3) [v]alues

transcend specific actions and situations...; (4) [v]alues serve as standards or criteria...; (5) [v]alues are ordered by importance...to form a system of priorities; and (6) [t]he relative importance of values guide action.” (Schwartz 2006, p. 143). Finally, the theory of cultural value orientations is widely used in the social sciences literature. Between 1988 and 2000, the first wave of SVS studies collected survey data from multiple countries around the globe. Initial wave gathered data from 80 samples of schoolteachers representing 58 national groups as well as from 115 samples of college students from 64 national groups. Each sample ranged between 180 and 280 participants. In multicultural countries, data were collected from the dominant cultural group of citizens. Between 2001 and 2018, the estimates from the first wave of studies were extended to new countries in the second wave of studies, which also validated and cross-checked previous results for selected countries by Schwartz and his coauthors as well as by other researchers, revealing no substantial shifts in estimates (e.g. Schwartz *et al.* 2010 ; Piurko *et al.* 2011 ; Schwartz & Sortheix 2018). By 2018, the comprehensive database of SVS results contained data from over 75,000 participants representing 74 countries. For our analysis, we use the comprehensive cultural value orientations dataset based on the SVS results from these 74 countries, which was provided to us by Professor Shalom H. Schwartz at the end of 2018.<sup>4</sup> Section 2.2 offers further description of the SVS as well as explains the methodology behind the calculation of cultural value orientations’ estimates from the SVS scores.

Our study also contributes to the *literature on human values and security governance*. A link between human values and regulations was established in research of Norman Feather, who used RVS and SVS approaches in direct and modified forms as well as a number of other measurements and tools linking the results of these surveys and measures to justice-related and regulatory behavior in a wide variety of empirical psychological studies (see e.g. Feather 1994; Feather & Boeckmann 2013; Strelan *et al.* 2016; Berndsen & Feather 2016). Yet, the link between human values and regulation in cyberspace has not been established in the previous literature. This study offers a framework which substantiates this link.

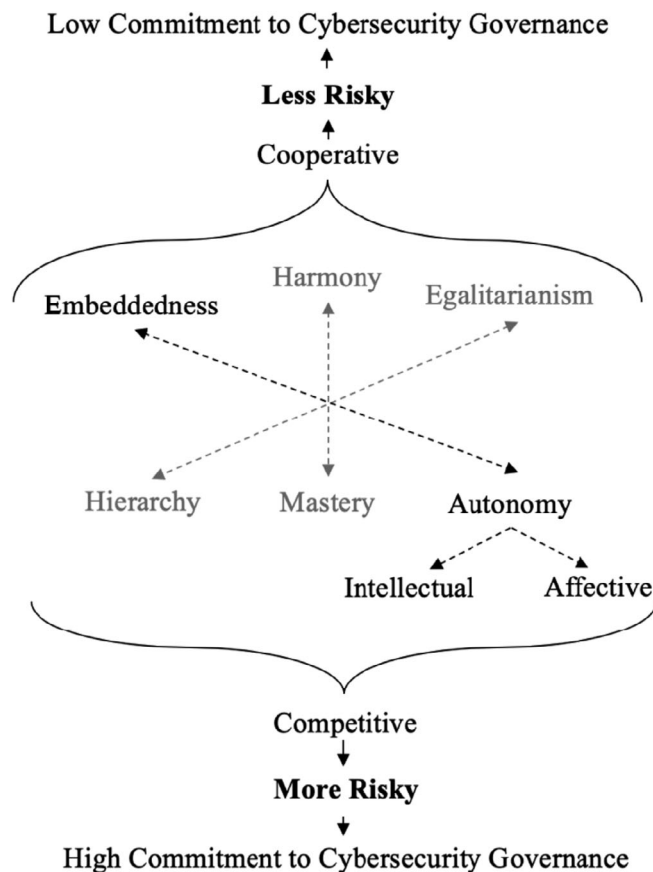
The main difference between cyberspace in the current globalized digital economy and traditional (noncyber or physical) spaces (where the cultural value orientations theory was applied so far) is that in the current digitized world with rapid flow of information across the globe, cultural differences become more and more difficult to detect. According to Rokeach (1973), even though values are relatively robust constructs, they may change throughout the human lifetime and may also exhibit a significant degree of heterogeneity across different domains. Yet, as long as our measures of human values for a particular country are based on values elicited from both the younger and the older generations (this is one of the most attractive features of the SVS data used in the study), it is natural to assume that, on average, such measures will be quite robust and accurate.

## 2.2. Human values-based framework for cybersecurity governance

Our framework depicted on Figure 1 is grounded in the Schwartz theory of cultural value orientations (see Schwartz 2006 for a detailed overview). As described above, Schwartz theory of cultural value orientations is based on three fundamental problems important for the formation of human values. We can define these problems as Social problem, Responsibility problem, and Nature problem.

- Society problem: the problem of coexistence between an individual and a group (highlighted by Embeddedness vs. Autonomy dichotomy).
- Responsibility problem: the problem of coexistence between an individual and social fabric responsibilities (highlighted by Egalitarianism vs. Hierarchy dichotomy).
- Nature problem: the problem of coexistence between human beings and nature (highlighted by Harmony vs. Mastery dichotomy).

Using dichotomies between Embeddedness and Autonomy, Egalitarianism and Hierarchy, as well as Harmony and Mastery, we first consider whether all three dichotomies may have an important impact in the digital space, specifically, when we consider cybersecurity issues. It is easy to notice that Social problem (captured by the Embeddedness and Autonomy dichotomy) plays a more important role for cyber spaces than the other two problems as it relates to the general issues of an individual’s place within the society. We all have individual and social experiences in the digital world as different people have different habits with regard to their cyber activities (such as sharing personal data via social media, enjoying a conversation with other people, etc.). Therefore, the



**Figure 1** Human values-based framework for cybersecurity regulation.

issues relevant to Embeddedness and Affective as well as Intellectual Autonomy, and values associated with them, are very important in the digital domain.

Responsibility problem (measured by Egalitarianism versus Hierarchy) is unlikely to impact on regulation of cyber space because it defines societal rankings for different strands of human life. Yet, one of the most interesting aspects of the use of the Internet as well as the human digital life is that hierarchical structures are rare in digital domain in a sense that when users are communicating or engaging with certain services online, they have equal social standing within the digital world. Of course, hierarchies may develop in digital communities over time but the starting position for the majority of people in the digital domain is very close to the egalitarian world.

Finally, the Nature problem is likely to have least (if any) impact in the digital setting. Of course, the Nature problem is important for many people as many of us are concerned with the use of environmental resources for technological purposes. However, people are unlikely to directly link the use of digital technology to environmental outcomes. For example, many of us are concerned about our personal carbon footprint which may affect our decisions about flying (because, as humans we see a direct link between the act of flying and generation of carbon footprint); yet, when we write an email, we rarely think of the consequences of our use of the digital technology, which is necessary to write that email, for the environment.

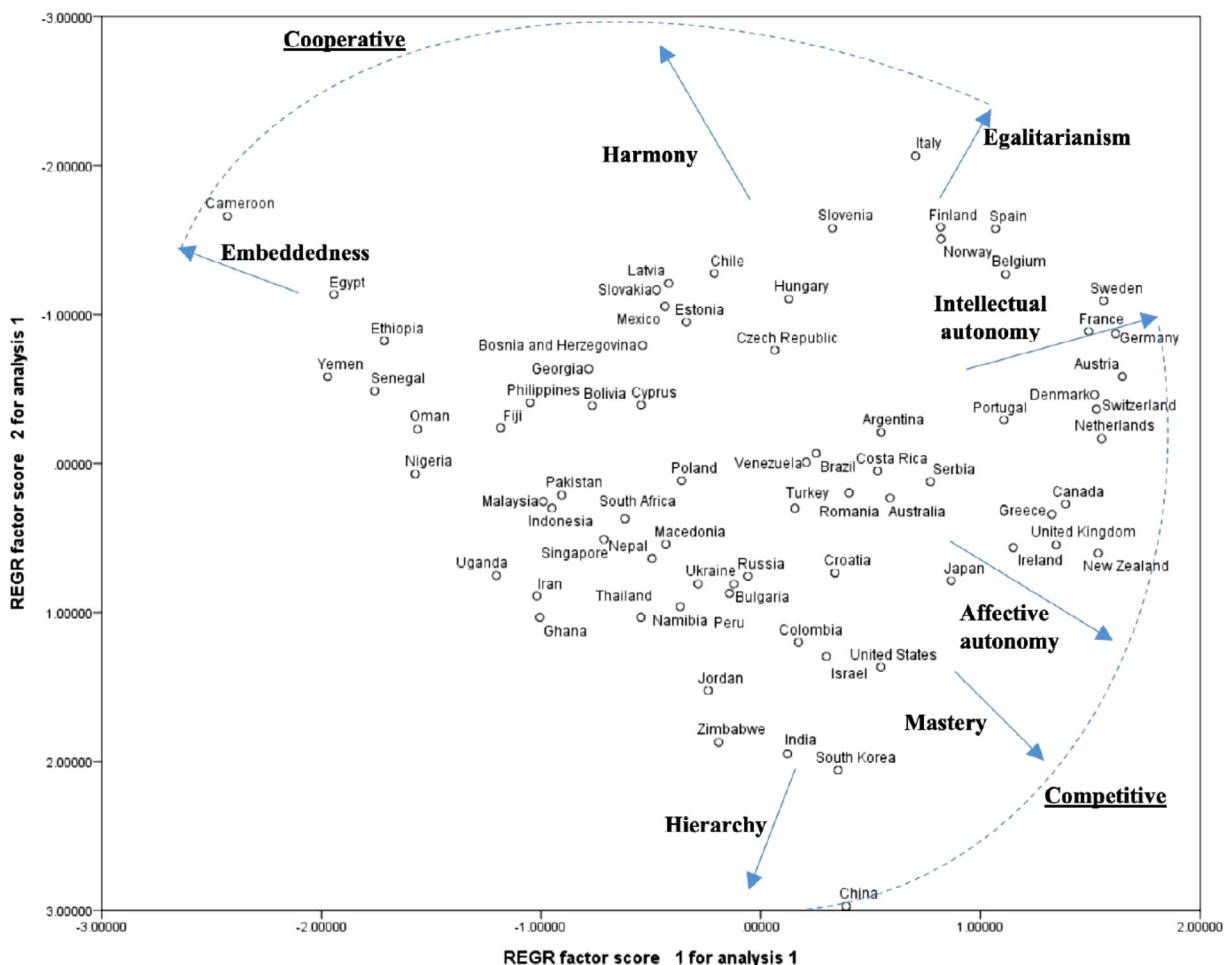
This leads us to the intermediate conjecture that Embeddedness and Autonomy are likely to be most important value construct for the digital domain, and, therefore, for cybersecurity. On Figure 1, therefore, Egalitarianism, Hierarchy, Harmony, and Mastery are shown in gray, whereas Embeddedness and Autonomy (both Affective and Intellectual) are shown in black. This leaves us with two major “poles” of human values. One of these poles is defined by Hierarchy, Mastery, and Autonomy constructs (of which, we expect Autonomy to be the most pronounced in the digital domain) and is mostly consistent with individual-based, more challenge-oriented value structure which we label the *Competitive* social human values pole; whereas the latter pole is defined by Embeddedness, Harmony, as well as Egalitarianism (of which, Embeddedness is likely to be most pronounced in

cyber spaces) and primarily associated with collective-based, more challenge-smoothing value structure which we label the *Cooperative* social human values pole.

In order to link Cooperative and Competitive poles to cybersecurity, one needs to consider the relative propensity to engage in risk-taking behavior online by nations from each pole (see Fig. 1).

There is considerable literature linking *attitudes toward risk* in “traditional” (noncyber) domains (such as health, environment, construction, finance, insurance, and conflict) as well as *behavior under risk* in these “traditional” domains to *values* (see e.g. Schelling 1985; Jones-Lee 1991, 1992; Carthy et al 1998; Slovic 2000; Sustain 2002; Wolff 2002; Pidgeon et al. 2003; and Posner 2004). Considering the nature and qualities of the polarized value constructs, we can anticipate that nations leaning toward the *Competitive* human values pole are prone to engaging into more risk seeking behavior in all domains including in cyberspace. At the same time, nations gravitating toward the *Cooperative* human values pole are more likely to exhibit risk averse behavior in all domains including cyberspace (see Fig. 1).

This conjecture is supported by extensive literature measuring risk attitudes across multiple cultures. Figure 2 shows a comprehensive mapping of 74 countries in the Schwartz dataset against the two poles identified by our framework on Figure 1 as well as relative to each other (see Fig. 2). This mapping is obtained by conducting a dimensional reduction factor analysis with 7 dimensions (Embeddedness, Affective and Intellectual Autonomy, Harmony, Mastery, Egalitarianism, and Hierarchy) to extract two principal orthogonal components using varimax rotation on all dimensions, which allows us to represent relationships between cultures in a two-dimensional space.



**Figure 2** Relative mapping of countries to poles and to each other. Our Figure 2 provides an identical relative mapping to that reported in Schwartz (2006) on Figure 4 (Schwartz 2006, p. 156), although Schwartz used data collected between 1988 and 2006 and applied the multidimensional scaling technique (Goldreich & Raveh 1993) rather than a dimensional reduction factor analysis used by us.

Note that our approach (shown on Fig. 1) allows for the *relative* rather than *absolute* comparisons. Also, relative rather than absolute relationships between countries are captured on Figure 2. Even though nations are unlikely to be unambiguously placed in either one pole area or the other, the proposed framework can, nevertheless, distinguish between predictions for different nations as those nations leaning toward the Competitive pole (in relative terms) can always be clearly distinguished from those gravitating toward the Cooperative pole (in relative terms). As long as a ranking of nations can be obtained in terms of their relative proximity to the poles (this ranking can be obtained from the SVS scores as shown on Fig. 2), our framework allows us to make meaningful predictions.

Let us take an example of three countries: United States, United Kingdom, and China. Figure 2 shows that according to the value orientations constructs, China is relatively closer to the Competitive pole (located at the bottom right corner of the figure) than United States and United Kingdom, and United States is located closer to the Competitive pole than United Kingdom. Therefore, if our conjecture is correct, Chinese citizens should be relatively more risk taking compared to the Americans and, in turn, Americans should be more risk taking than British citizens. In noncyber domains, Chinese study participants were shown to be more risk taking compared to American study participants using economic experiments (e.g. Hsee & Weber 1999); and American population was shown to be more risk taking in financial domain than the UK population (e.g. Ferreira 2018). In the digital domain, Kharlamov *et al.* (2018) demonstrated using representative samples of both populations that Americans are (on average) more risk taking than British people. Pogrebna and Skilton (2019) reported on further studies which found Chinese people to be more risk taking in cyber spaces than American people and, in turn, American people were more risk taking than British people over a wide variety of cyber risks.<sup>5</sup>

As Competitive pole nations are “riskier” than Cooperative nations in the digital space (i.e. more likely to engage in risk-taking behaviors online), we hypothesize that Competitive nations would try to alleviate the potential risks to cybersecurity by regulation and governance of cyber space. At the same time, Cooperative nations are less likely to exhibit risk-taking behavior online and are, therefore, viewed by their governments as more “self-regulating.” Therefore, these nations adopt more informal approach to solving cybersecurity problems.

Recall that we expect Embeddedness and Autonomy to play particularly important role for national behavior in cyber spaces. This allows us to hypothesize that nations who score relatively high on (Affective or Intellectual) Autonomy will be more efficient in cybersecurity regulation (because they need to offset potentially negative effects of risk-taking behavior of their citizens), whereas nations who score relatively high on Embeddedness will be less efficient in cybersecurity regulation (because their citizens are more likely to be risk averse in digital spaces). More specifically, we anticipate nations with high Autonomy scores to be more risk seeking in cyberspace, we also anticipate that their behavior in cyberspace will particularly depend on constructs which are a matter of individual choice (e.g. such as individual ethical code of conduct). In such *Competitive* nations, individuals will not view their rights in cyberspace (such as, e.g. the right to privacy or personal data protection) as inherent human rights due to the individual-based and more challenge-oriented nature of the value system. This means that individual behavior in cyberspace for representatives of these nations will, in many ways, depend on their personal understanding of the ethical principles behind various modes of conduct they can choose from. Such behavior will generate risks which, in turn, would need a more effective and precise regulation.

At the same time, in nations which score high on Embeddedness, the nature of the human values system implies that behavior in cyberspace will be guided more by societal cultural principles. Risk attitudes in cyberspace for such *Cooperative* nations are more likely to be guided by constructs of collective nature. Such nations will, therefore, be less efficient in governing cyberspaces as they would expect alternative societal instruments to act in place of regulation.

### 2.3. Measures and data

In order to test our framework (proposed on Fig. 1), we combine three datasets: (i) the large-scale dataset with measures of cultural value orientations; (ii) the Global Cybersecurity Index dataset; and (iii) the Worldwide Governance Indicators dataset.

As described in Section 2.2, we obtained the relative mapping of nations from the previous comprehensive and large-scale studies conducted by Professor Shalom H. Schwartz and his research team, which allowed us to determine the relative proximity of each nation to the Cooperative and Competitive poles. Raw scores for each value orientation measure were used in our analysis.<sup>6</sup>



In order to link cultural value orientations to the cybersecurity governance, we use the Global Cybersecurity Index (GCI). The GCI is a composite index, created and compiled by the International Telecommunications Union (ITU), which consists of 25 indicators partitioned into five pillars. The ITU's General Model Framework explains the difference between the five pillars as follows (ITU 2018, p. 4):

- 1 Legal pillar includes "...[m]easures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime."
- 2 Technical pillar consists of "...[m]easures based on the existence of technical institutions and frameworks dealing with cybersecurity."
- 3 Organizational pillar incorporates "...[m]easures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level."
- 4 Capacity Building pillar contains "...[m]easures based on the existence of research and development, education and training programs; certified professionals and public sector agencies fostering capacity building."
- 5 Cooperation pillar is based on "...[m]easures based on the existence of partnerships, cooperative frameworks and information sharing networks."

Based on these five pillars, five subcoefficients (one per each pillar) are added up to obtain one (Total) GCI coefficient. According to ITU, the GCI allows to measure "cybersecurity commitment" in different countries.<sup>7</sup> The index allows to understand the relative strength of commitment to cybersecurity governance and regulation in different parts of the world from hundreds of countries. Generally, the higher the index, the more committed a nation is to regulating and governing cybersecurity. We used the GCI values calculated by the ITU for the year 2017 (total as well as by pillar coefficients were available to us).<sup>8</sup>

Additionally, in order to compare governance and regulation of cybersecurity to governance and regulation in other traditional domains, we also used a set of additional indicators from the Worldwide Governance Indicators (WGI) 2017 (see Kaufmann *et al.* 1998 for the summary of the indicators methodology) which provided governance indicators for more than 200 states. According to Kaufmann *et al.* (2010, p. 1), "the six aggregate indicators [in WGI] are based on over 30 underlying data sources reporting the perceptions of governance by a large number of survey respondents and expert assessments worldwide."<sup>9</sup> The WGI project allowed us to use the following governance measures (indicators) for traditional domains (Kaufmann *et al.* 2010, p. 3):

- Voice and Accountability "reflects perceptions of the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media."
- Political Stability and Absence of Violence "measures perceptions of the likelihood of political instability and/or politically-motivated violence, including terrorism."
- Government Effectiveness "reflects perceptions of the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies."
- Regulatory Quality "reflects perceptions of the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development."
- Rule of Law "reflects perceptions of the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, property rights, the police, and the courts, as well as the likelihood of crime and violence."
- Control of Corruption "reflects perceptions of the extent to which public power is exercised for private gain, including both petty and grand forms of corruption, as well as capture of the state by elites and private interests."

Combining the data allowed us to compile a comprehensive dataset of various governance measures (both from the CGI data and the WGI data) and associated human values' constructs from the SVS survey for 74 countries around the globe. We use this dataset for our analysis.

Our approach and existence of the relevant measures allow us to formulate the following testable hypotheses:

**Table 1** Correlation between value orientation items and governance in cybersecurity and traditional domains

Human value constructs	GCI (total)	World Governance Indicators						
		Voice and Accountability	Political Stability and Absence of Violence /Terrorism	Government Effectiveness	Regulatory Quality	Rule of Law	Control of Corruption	
Embeddedness	-0.414*** (0.000)	-0.790*** (0.000)	-0.615*** (0.000)	-0.731*** (0.000)	-0.704*** (0.000)	-0.707*** (0.000)	-0.672*** (0.000)	
Affective	-0.413*** (0.000)	-0.762*** (0.000)	-0.614*** (0.000)	-0.730*** (0.000)	0.693*** (0.000)	-0.698*** (0.000)	-0.701*** (0.000)	
Autonomy	0.444*** (0.000)	0.707*** (0.000)	0.553*** (0.000)	0.719*** (0.000)	0.647*** (0.000)	0.686*** (0.000)	0.668*** (0.000)	
Intellectual	0.450*** (0.000)	0.670*** (0.000)	0.566*** (0.000)	0.724*** (0.000)	0.667*** (0.000)	0.694*** (0.000)	0.713*** (0.000)	
Autonomy	0.333*** (0.002)	0.703*** (0.000)	0.559*** (0.000)	0.644*** (0.000)	0.622*** (0.000)	0.626*** (0.000)	0.597*** (0.000)	
Harmony	0.345** (0.003)	0.685*** (0.000)	0.563*** (0.000)	0.662*** (0.000)	0.613*** (0.000)	0.632*** (0.000)	0.628*** (0.000)	
Mastery	0.099 (0.202)	0.442*** (0.000)	0.337** (0.002)	0.312** (0.003)	0.330** (0.002)	0.311** (0.004)	0.287*** (0.007)	
Egalitarianism	0.107 (0.365)	0.401*** (0.000)	0.290* (0.012)	0.285* (0.014)	0.290* (0.012)	0.288* (0.013)	0.270* (0.020)	
Hierarchy	-0.067 (0.286)	-0.019 (0.438)	-0.057 (0.315)	-0.031 (0.395)	-0.051 (0.334)	-0.048 (0.343)	-0.066 (0.287)	
	-0.039 (0.739)	-0.059 (0.619)	-0.034 (0.773)	-0.040 (0.733)	-0.071 (0.550)	-0.068 (0.563)	-0.089 (0.451)	
	0.119 (0.156)	0.617*** (0.000)	0.349*** (0.001)	0.394*** (0.000)	0.424*** (0.000)	0.426*** (0.000)	0.466*** (0.000)	
	0.119 (0.311)	0.575*** (0.000)	0.300** (0.010)	0.388*** (0.001)	0.397*** (0.001)	0.414*** (0.000)	0.472*** (0.000)	
	-0.128 (0.139)	-0.566*** (0.000)	-0.487*** (0.000)	-0.437*** (0.000)	-0.442*** (0.000)	-0.502*** (0.000)	-0.464*** (0.000)	
	-0.090 (0.446)	-0.548*** (0.000)	-0.426*** (0.000)	0.390*** (0.001)	0.413*** (0.000)	-0.445*** (0.000)	-0.444*** (0.000)	

\*Significant at 0.05 level. \*\*Significant at 0.01 level. \*\*\*Significant at 0.001 level.

Spearman correlation is reported in the upper row and Pearson correlation is reported in the lower row against each human value construct (listed in the first column of the table).

Hypothesis 1: Nations which score high on Embeddedness are less committed to regulation and governance of cybersecurity (High Embeddedness scores are associated with low GCI index).

Hypothesis 2: Nations which score high on Autonomy are more committed to regulation and governance of cybersecurity (High Autonomy scores are associated with high GCI index).

### 3. Analysis and results

In this section, we will look at human values mapping according to Schwartz's theory and then overlay this mapping with the total GCI as well as WGI indicators. In the first instance, we conduct a simple correlation analysis using Spearman and Pearson correlation tests. Results of the test are presented in Table 1.

The table shows that Embeddedness is highly negatively correlated with GCI, but GCI is positively correlated with both Autonomy measures (Affective and Intellectual Autonomy). As anticipated, other indicators (Hierarchy, Egalitarianism, Harmony, and Mastery) do not produce strong correlations with GCI. Interestingly, WGI measures which refer to traditional regulation and governance domains (Voice and Accountability, Political Stability and Absence of Violence, Government Effectiveness, Regulatory Quality, Rule of Law, and Control of Corruption) are also positively correlated with Autonomy and negatively correlated with Embeddedness. Yet, unlike GCI, WGI constructs are positively correlated with Egalitarianism but negatively correlated with Hierarchy. Also, the WGI measures are positive correlated with Harmony.

Therefore, at least at the level of simple correlations, our hypotheses are correct: high Embeddedness is associated with low governmental commitment to regulate cybersecurity, whereas high Autonomy is associated with high governmental commitment to regulate cybersecurity. In order to test our hypotheses further, we conduct a series of ordinary least squares (OLS) regressions with GCI total score as well as individual score for each of the GCI pillars: Legal, Technical, Organizational, Capacity building, and Cooperation. In order to control for economic development of countries under consideration, we include a control variable of the national income group (the country can belong to one of the following four income groups according to the World Bank Statistics: Low Income, Lower Middle Income, Higher Middle Income, and High Income). We use this variable to cluster countries by national incomes. As the number of observations in our sample is limited ( $N = 74$  countries) and the value orientation measures, by construction, represent antipodes (in other words, these measures are correlated between each other), each cell of Table 2 represents results (coefficient and robust standard error) for regressions where CGI constructs are predicted using value orientation constructs.

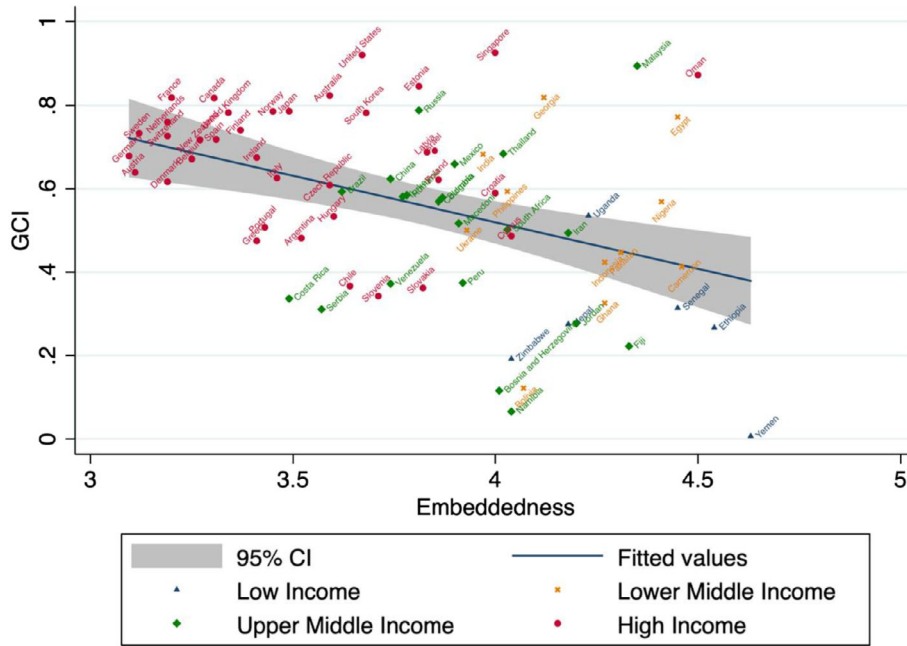
Table 2 shows that even when the economic development level of each country is taken into account by our analysis (using the national income group control variable), we find that Embeddedness and Autonomy are the

**Table 2** Results of a series of clustered OLS regressions predicting the GCI constructs using value orientation constructs

Independent variable	GCI					
	Legal	Technical	Organizational	Capacity building	Cooperation	Total
Embeddedness	-0.022 <sup>#</sup> (0.090)	-0.033* (0.090)	-0.183 (0.085)	-0.220* (0.068)	-0.170* (0.044)	-0.223* (0.070)
Affective Autonomy	0.189* (0.052)	0.222* (0.063)	0.171* (0.052)	0.197** (0.027)	0.156*** (0.010)	0.186* (0.036)
Intellectual Autonomy	0.165 (0.095)	0.299 <sup>#</sup> (0.101)	0.158 (0.096)	0.195 <sup>#</sup> (0.080)	0.157 <sup>#</sup> (0.054)	0.193 <sup>#</sup> (0.079)
Harmony	0.101 (0.129)	0.212 (0.134)	0.064 (0.159)	0.003 (0.180)	0.024 (0.068)	0.080 (0.127)
Mastery	-0.092 (0.150)	-0.081 (0.037)	-0.001 (0.060)	0.024 (0.088)	-0.109* (0.030)	-0.054 (0.048)
Hierarchy	-0.067 (0.033)	-0.109 (0.084)	-0.041 (0.054)	0.052 (0.108)	-0.052 (0.029)	-0.044 (0.058)
Egalitarianism	0.077 (0.067)	0.238** (0.029)	0.046 (0.037)	0.071 (0.118)	0.058 (0.101)	0.096 (0.055)

\*Significant at 0.05 level. \*\*Significant at 0.01 level. \*\*\*Significant at 0.001 level. <sup>#</sup>Significant at 0.1 level.

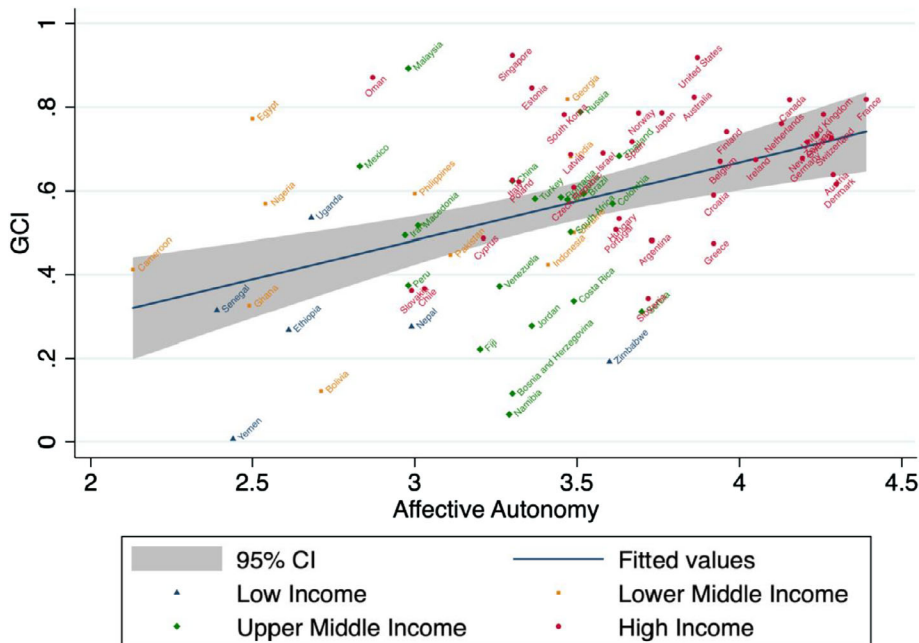
Error terms (reported in brackets) are clustered based on four income groups: Low Income, Lower Middle Income, Higher Middle Income, and High Income.



**Figure 3** Embeddedness versus the Global Cybersecurity Index.

only two variables which are consistently significant for the majority of the GCI pillars as well as for the total GCI coefficient.<sup>10</sup> Table 2 reveals several interesting additional results. First, it demonstrates that between the two autonomy measures, Affective Autonomy seems to be the more important determinant of our cybersecurity governance measure.

Specifically, in every column of Table 2, the Affective Autonomy coefficient has higher significance than the Intellectual autonomy coefficient. Moreover, in the majority of columns, the values of the Affective Autonomy coefficients are higher than those of the Intellectual autonomy. This suggests that countries, where citizens believe that pursuing own satisfaction is important, tend to concentrate more on regulating cybersecurity than countries, where citizens find pursuing own intellectual goals important.



**Figure 4** Affective Autonomy versus the Global Cybersecurity Index.

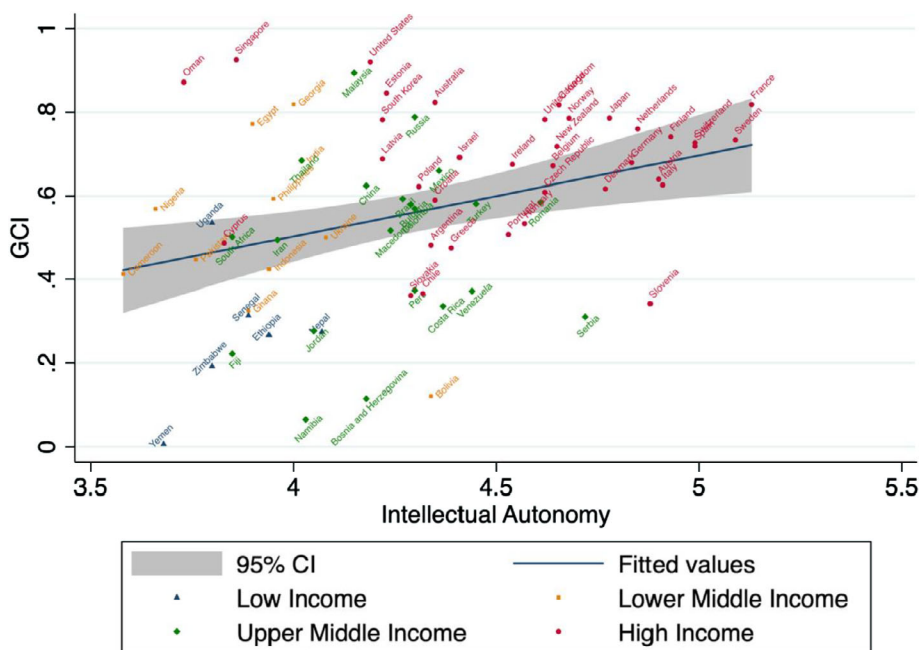


Figure 5 Intellectual Autonomy versus the Global Cybersecurity Index.

In order to provide a better visualization of this result, we also plot Figures 3–5.

Figures 3–5 show the correlation between the GCI as well as Embeddedness, Affective Autonomy, and Intellectual Autonomy, respectively. Income control is captured by different shapes and colors of the observations. These figures demonstrate strong correlation between Embeddedness and CGI as well as between Affective Autonomy and CGI, yet, despite the visible correlation between CGI and Intellectual Autonomy, it is obvious that the slope of the regression line on Figure 5 is lower (less steep) than that on Figure 4. This means that, of the two Autonomy measures, Affective Autonomy plays a more important role for cybersecurity regulation.

Additionally, Table 2 also shows occasional correlations between individual pillars of GCI and the value orientation constructs. Specifically, the Technical pillar has a strong and positive correlation with Egalitarianism and Cooperation pillar is (statistically significantly) negatively correlated with Mastery.

#### 4. Conclusion

Using information technology, individuals on a daily basis are subjected to a considerable amount of risk, whether voluntarily or involuntarily in both digital and noncyber environments. Understanding how people deal with risk in cyberspace is of extreme importance as responsible use of technology is one of the most important problems facing businesses and governments in the modern global community. Notorious exhibits of the irresponsible use causing harm to large numbers of citizens (such as the Cambridge Analytica case) tell us that regulation of the Internet (as one of the major technological developments of the modern global society) is necessary.

Although much research is devoted to the development of risk measures in digital domains (e.g. Kharlamov *et al.* 2018; Pogrebna and Skilton 2019), it is equally important to understand the origins of human behavior in cyber spaces as well as to analyze how regulatory frameworks develop around human values as well as human behavioral patterns.

This article proposes that human values lie at the core of the human risk-taking behavior in the digital space, which, in turn has a direct impact on the way in which digital domain is regulated. Using an example of cybersecurity, we develop a framework which links human values and cybersecurity regulation by making inferences about the connections between human values and risk-taking behavior. We demonstrate that empirical tests provide a robust support of this framework.

Our contribution extends not only the literature on measurement of human values (e.g. Schwartz 1992; Schwartz 2006) but also on regulation and governance of security (e.g. Shearing & Johnston 2013) as well as on

human values and security governance (e.g. Feather & Boeckmann 2013). We show how combining all three streams of literature can yield a new cross-disciplinary framework for understanding commitment toward regulation and governance of cybersecurity across different nations.

It is left to future research to explore more detailed reasons behind the cultural differences observed in cyberspace. Yet, it appears that human values shape an important determinant of the heterogeneity for cyber-related governance and regulation across the globe, which should not go overlooked.

## Endnotes

- 1 For the detailed mapping of heterogeneity in the Internet regulation around the globe, see for example, <http://www.ipvn.net>.
- 2 All questions were asked in respondents' native language. Over the years, the SVS increased from 56 value indicators to 57 value indicators. Recently, 58th value indicator was added to the survey. The Appendix to this article includes detailed description of each value instrument.
- 3 This is why the cultural value orientations theory is often referred to as a seven-dimensional instrument.
- 4 We are very grateful to Professor Schwartz for sharing his lifetime work with our team. As explained above, SVS grew over the years from 56 to 57 and then to 58 indicators. In the dataset, provided to us by Professor Schwartz, respondents were subjected either to 56 (majority of samples) or to 57 indicators (minority of samples). Professor Schwartz's team then applied a sophisticated adjustment procedure to make sure that: (i) the sample from 56-indicator survey and 57-indicator survey were comparable as well as; and (ii) that data collected from different countries were appropriately cleansed and debiased (see <http://www.crossculturalcentre.homestead.com> for more detail). Considering that these adjustments are not trivial, it was important for us to use the original dataset collected by Professor Schwartz's team rather than collect our own data as we did not want to misrepresent or misinterpret the measures. Additionally, any new dataset would have been significantly smaller than the multinational dataset provided by Professor Schwartz.
- 5 For a concise summary of these results, please see <https://www.forbes.com/sites/charlestowersclark/2018/11/09/relaxed-anxious-ignorant-our-attitudes-towards-cybersecurity-are-making-the-problem-worse/#31818d14673a>.
- 6 We are very grateful to Professor Schwartz for his value orientations dataset.
- 7 See [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf) for more detail.
- 8 We are very grateful to the ITU, especially to Maxim Kushtuev for providing a detailed GCI dataset to our research team.
- 9 See <http://info.worldbank.org/governance/wgi/#home> for more detail.
- 10 Note that this article does not intend to suggest that a population of a particular country should be viewed as a homogeneous entity: various population groups may exhibit different cultural values. Nevertheless, our analysis shows that the human value-based argument appears to be valid at a general level.

## References

- Allsop J (2017) Values in Law: How they Influence and Shape Rules and the Application of Law. *Brief* 44(2), 49.
- Berndsen M, Feather NT (2016) Reflecting on Schadenfreude: Serious Consequences of a Misfortune for which One Is Not Responsible Diminish Previously Expressed Schadenfreude; the Role of Immorality Appraisals and Moral Emotions. *Motivation and Emotion* 40(6), 895–913.
- Carthy T, Chilton S, Covey J *et al.* (1998) On the contingent valuation of safety and the safety of contingent valuation: part 2-The CV/SG "chained" approach. *Journal of Risk and Uncertainty* 17(3), 187–214.
- Clark D, Berson T, Lin HS (2014) At the Nexus of Cybersecurity and Public Policy. *Computer Science and Telecommunications Board, National Research Council*. The National Academies Press, Washington, DC.
- Crawford A (2006) Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security. *Theoretical Criminology* 10(4), 449–479.
- Feather NT (1982) *Expectations and Actions: Expectancy-Value Models in Psychology*. Lawrence Erlbaum Assoc Incorporated, Hillsdale, NJ.
- Feather NT (1994) Human Values and their Relation to Justice. *Journal of Social Issues* 50(4), 129–151.
- Feather NT, Boeckmann RJ (2013) Perceived Legitimacy of Judicial Authorities in Relation to Degree of Value Discrepancy with Public Citizens. *Social Justice Research* 26(2), 193–217.
- Ferreira M (2018) Risk Seeker or Risk Averse? CrossCountry Differences in Risk Attitudes Towards Financial Investment. *The Behavioral Economics Guide* 2018, 86–95.
- Goldreich Y, Raveh A (1993) Coplot Display Technique as an Aid to Climatic Classification. *Geographical Analysis* 25(4), 337–353.

- Hillson D, Murray-Webster R (2012) *Understanding and Managing Risk Attitude*, 2nd edn. Routledge, Taylor and Francis, New York, NY.
- Hsee CK, Weber EU (1999) Cross-National Differences in Risk Preference and Lay Predictions. *Journal of Behavioral Decision Making* 12(2), 165–179.
- International Telecommunications Union (2018) *Global Cybersecurity Index, General Framework Brief*. [Last accessed 10 September 2019] Available from URL: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf).
- Johnsten L, Shearing C (2003) *Governing Security: Explorations in Policing and Justice*, pp. 281–297. Routledge, New York.
- Jones-Lee MW (1991) Altruism and the Value of Other people's Safety. *Journal of Risk and Uncertainty* 4(2), 213–219.
- Jones-Lee MW (1992) Paternalistic Altruism and the Value of Statistical Life. *The Economic Journal* 102(410), 80–90.
- Kaufmann D, Kraay, A, Mastruzzi, M (2010) The Worldwide Governance Indicators: Methodology and Analytical Issues. Policy Research Working Paper No. WPS 5430. World Bank. [Last accessed 10 Sep 2019.] Available from URL: <https://openknowledge.worldbank.org/handle/10986/3913>.
- Kharlamov A, Jaiswal A, Parry G, Pogrebna G (2018) A Cyber Domain-Specific Risk Attitudes Scale to Address Security Issues in the Digital Space, mimeo. <https://doi.org/10.13140/RG.2.2.31408.05122/2>.
- Loader I, Walker N (2004) State of Denial? *Rethinking the Governance of Security, Punishment & Society* 6(2), 221–228.
- Pidgeon N, Kasperson RE, Slovic P (2003) *The Social Amplification of Risk*. Cambridge University Press, Cambridge, United Kingdom.
- Piurko Y, Schwartz SH, Davidov E (2011) Basic Personal Values and the Meaning of Left-Right Political Orientations in 20 Countries. *Political Psychology* 32(4), 537–561.
- Pogrebna G, Skilton M (2019) *Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*. Springer, Cham, Switzerland. ISBN 978-3-030-13527-0. <https://doi.org/10.1007/978-3-030-13527-0>.
- Posner RA (2004) *Catastrophe: Risk and Response*. Oxford University Press, New York, NY.
- Rokeach M (1973) *The Nature of Human Values*. Free Press, New York, NY.
- Schelling TC (1985) *Choice and Consequence*. Harvard University Press, Cambridge, MA.
- Schwartz SH (1992) Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. *Advances in Experimental Social Psychology*, 25, 1–65. [https://doi.org/10.1016/S0065-2601\(08\)60281-6](https://doi.org/10.1016/S0065-2601(08)60281-6).
- Schwartz SH (2006) A Theory of Cultural Value Orientations: Explication and Applications. *Comparative Sociology* 5(2), 137–182.
- Schwartz SH, Sortheix F (2018) Values and Subjective Well-Being. In: Diener E, Oishi S, Tay L (eds) *Handbook of Well-Being*, pp. 1–25. Noba Scholar, Salt Lake City, UT. [Last accessed 10 September 2019.] Available from URL: <http://www.nobascholar.com/chapters/51>.
- Schwartz SH, Caprara GV, Vecchione M (2010) Basic Personal Values, Core Political Values, and Voting: A Longitudinal Analysis. *Political Psychology* 31(3), 421–452.
- Shearing CD, Johnston L (2013) *Governing Security: Explorations of Policing and Justice*. Routledge, New York, NY.
- Slovic P (2000) What Does it Mean to Know a Cumulative Risk? Adolescents' Perceptions of Short-Term and Long-Term Consequences of Smoking. *Journal of Behavioral Decision Making* 13(2), 259–266.
- Strelan P, McKee I, Feather NT (2016) When and how Forgiving Benefits Victims: Post- Transgression Offender Effort and the Mediating Role of Deservingness Judgements. *European Journal of Social Psychology* 46(3), 308–322.
- Sunstein CR (2002) The law of group polarization. *Journal of Political Philosophy* 10(2), 175–195.
- Wolff J (2002) Railway Safety and the Ethics of the Tolerability of Risk. *Railway Safety Standards Board Study*. [Last accessed 10 September 2019.] Available from URL: <https://pdfs.semanticscholar.org/a300/4b256f74a0cd49375c9d55faaa4c64058c66.pdf>.
- Wolff J (2006) Risk, Fear, Blame, Shame and the Regulation of Public Safety. *Economics & Philosophy* 22(3), 409–427.

## 5. APPENDIX

### Using Schwartz Value Survey to Measure Seven Cultural Value Orientations

We use data collected from 74 countries using the Schwartz Value Survey (SVS) which form proxies for seven cultural value orientations. Initially, SVS contained 56 indicators which were later extended to 57 indicators and then to 58 indicators. The most widely used SVS contains 57 indicators. Each indicator is a measure of a specific value. Table A provides a summary of all 57 indicators.

**Table A** Schwartz value survey indicators and their meaning

ID	SVS indicator	Meaning
1	EQUALITY	Equal opportunity for all
2	INNER HARMONY	At peace with myself
3	SOCIAL POWER	Control over others, dominance
4	PLEASURE	Gratification of desires
5	FREEDOM	Freedom of action and thought

(Continues)

Table A Continued

ID	SVS indicator	Meaning
6	A SPIRITUAL LIFE	Emphasis on spiritual not material matters
7	SENSE OF BELONGING	Feeling that others care about me
8	SOCIAL ORDER	Stability of society
9	AN EXCITING LIFE	Stimulating experiences
10	MEANING IN LIFE	A purpose in life
11	POLITENESS	Courtesy, good manners
12	WEALTH	Material possessions, money
13	NATIONAL SECURITY	Protection of my nation from enemies
14	SELF RESPECT	Belief in one's own worth
15	RECIPROCATION OF FAVORS	Avoidance of indebtedness
16	CREATIVITY	Uniqueness, imagination
17	A WORLD AT PEACE	Free of war and conflict
18	RESPECT FOR TRADITION	Preservation of time-honored customs
19	MATURE LOVE	Deep emotional and spiritual intimacy
20	SELF-DISCIPLINE	Self-restraint, resistance to temptation
21	PRIVACY	The right to have a private sphere
22	FAMILY SECURITY	Safety for loved ones
23	SOCIAL RECOGNITION	Respect, approval by others
24	UNITY WITH NATURE	Fitting into nature
25	A VARIED LIFE	Filled with challenge, novelty, and change
26	WISDOM	A mature understanding of life
27	AUTHORITY	The right to lead or command
28	TRUE FRIENDSHIP	Close, supportive friends
29	A WORLD OF BEAUTY	Beauty of nature and the arts
30	SOCIAL JUSTICE	Correcting injustice, care for the weak
31	INDEPENDENT	Self-reliant, self-sufficient
32	MODERATE	Avoiding extremes of feeling & action
33	LOYAL	Faithful to my friends, group
34	AMBITIOUS	Hard-working, aspiring
35	BROADMINDED	Tolerant of different ideas and beliefs
36	HUMBLE	Modest, self-effacing
37	DARING	Seeking adventure, risk
38	PROTECTING THE ENVIRONMENT	Preserving nature
39	INFLUENTIAL	Having an impact on people and events
40	HONORING OF PARENTS AND ELDERS	Showing respect
41	CHOOSING OWN GOALS	Selecting own purposes
42	HEALTHY	Not being sick physically or mentally
43	CAPABLE	Competent, effective, efficient
44	ACCEPTING MY PORTION IN LIFE	Submitting to life's circumstances
45	HONEST	Genuine, sincere
46	PRESERVING MY PUBLIC IMAGE	Protecting my "face"
47	OBEDIENT	Dutiful, meeting obligations
48	INTELLIGENT	Logical, thinking
49	HELPFUL	Working for the welfare of others
50	ENJOYING LIFE	Enjoying food, sex, leisure, and so forth
51	DEVOUT	Holding to religious faith and belief
52	RESPONSIBLE	Dependable, reliable
53	CURIOUS	Interested in everything, exploring
54	FORGIVING	Willing to pardon others
55	SUCCESSFUL	Achieving goals

*(Continues)*



**Table A** Continued

ID	SVS indicator	Meaning
56	CLEAN	Neat, tidy
57	SELF-INDULGENT	Doing pleasant things

**Notes:** Indicators are presented exactly as described in Schwartz, Shalom H. (2009). Draft Users Manual: Proper Use of the Schwarz Value Survey, version 14 January 2009, compiled by Romie F. Littrell. Auckland, New Zealand: Centre for Cross Cultural Comparisons, <http://www.crossculturalcentre.homestead.com>. In the latest version of SVS, one additional indicator was added (“OBSERVING SOCIAL NORMS” which means “to maintain face”). However, this indicator is not relevant for our study as it was not used in surveys which formed the dataset used in our article. In the SVS, each participant is presented with value indicators and their meanings (see Table A) in their native language and asked to rate the importance of each value indicator “as a guiding principle in [THEIR] life” on a four-fold scale, where the answer “of supreme importance” receives a score of 7, “important” receives a score of 3, “not important” receives a score of 0, and “opposed to my values” receives score of –1. Table B summarizes the way in which cultural value orientations are formed, that is, it shows the value indicators included in each cultural human value construct category.

**Table B** Composition of the cultural value orientation constructs

Human value constructs at a cultural level	SVS indicator IDs	SVS indicators included
Embeddedness	8, 11, 13, 15, 18, 20, 26, 32, 40, 46, 47, 51, 54, 56	SOCIAL ORDER; POLITENESS; NATIONAL SECURITY; RECIPROCATION OF FAVORS; RESPECT FOR TRADITION; SELF DISCIPLINE; WISDOM; MODERATE; HONORING OF PARENTS AND ELDERS; PRESERVING MY PUBLIC IMAGE; OBEDIENT; DEVOUT; FORGIVING; CLEAN
Affective Autonomy	4, 9, 25, 50, 57	PLEASURE; AN EXCITING LIFE; A VARIED LIFE; ENJOYING LIFE; SELF-INDULGENT
Intellectual Autonomy	5, 16, 35, 53	FREEDOM; CREATIVITY; BROADMINDED; CURIOUS
Harmony	17, 24, 29, 38	A WORLD AT PEACE; UNITY WITH NATURE; A WORLD OF BEAUTY; PROTECTING THE ENVIRONMENT
Mastery	23, 31, 34, 37, 39, 41, 43, 55,	SOCIAL RECOGNITION; INDEPENDENT; AMBITIOUS; DARING; INFLUENTIAL; CHOOSING OWN GOALS; CAPABLE; SUCCESSFUL
Hierarchy	3, 12, 27, 36, 39	SOCIAL POWER; WEALTH; AUTHORITY; HUMBLE; INFLUENTIAL
Egalitarianism	1, 30, 33, 45, 49, 52	EQUALITY; SOCIAL JUSTICE; LOYAL; HONEST; HELPFUL; RESPONSIBLE