ABIresearch | Global Cybersecurity Index

Published July 2, 2015

CYBERSECURITY INDEX OF INDICES

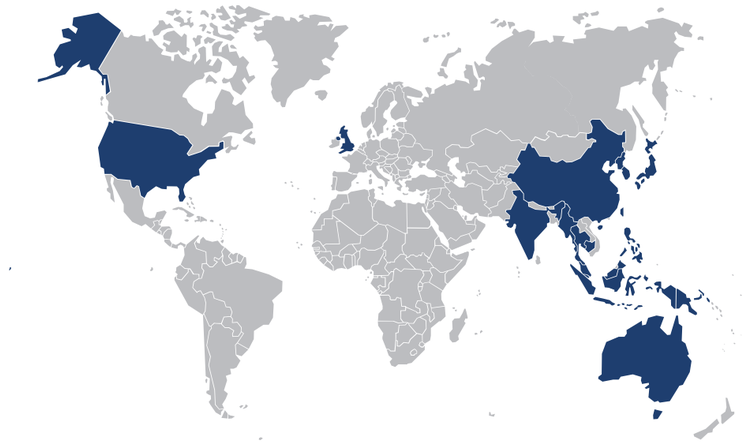
Cybersecurity development is a complex matter. Whether at the nation state level, or in an enterprise, various factors need to be taken into consideration and layered approach can provide more comprehensive coverage than single solutions. The application of cybersecurity is also a continuous process that needs to match ongoing cybercriminal activities and threat campaigns. As such, the measurement of security postures and progress over time are important elements to strengthening policies, evaluating risks and anticipating future scenarios. Various cybersecurity indices have been published in the past few years; yet not all measure the same capabilities. They can be broadly split into 3 major groups: indices for assessing countries' national postures, indices for assessing organizations, and indices for assessing threats. The three groups are presented below alongside current relevant indices.

1. 1. INDICES FOR ASSESSING COUNTRIES

Indices for assessing countries have been developed by international organizations and think tanks, often in partnership with private sector organizations. At the highest level, these indices look at policy and regulatory aspects, organizational measures, national strategies, and cooperative efforts among others. Some indices simply compare and contrast measures amongst countries, while others provide an index scoring based on indicators. Others still provide rankings based on the scoring. All offer valuable information on cybersecurity practices and gaps at the nation state level.

	Cyber Maturity	Cyber Threats	Score	Ranking	Index	Frame-work	Policy	Organiza-tional	Technical	Economical	Recommen-dations	Profiles
Global Cybersecurity Index	x		x	x	x		x	x				
Cyber Maturity in the Asia-Pacific Region	x		x		x		x	x				x
The Cyber Index: International Security Trends and Realities	x					x	x					x
Cybersecurity: The Vexed Question of Global Rules	x		x		x		x	x			x	x
Cybersecurity Policy Making at a Turning point	x					x	x	x				
Cyber Operations Maturity Framework	x	x				x		x				
Cyber Readiness Index 2.0	x		x		x		x			x		
Cyber Security Intelligence Index		x			x				x		x	
Index of Cybersecurity		x			x				x			
Cybersecurity Index		x	x		x				x			
Gibson Index		x			x				x			
Information Risk Maturity Index 2014	x		x		x			x				
Risk and Responsibility in a Hyperconnected World	x	x				x		x		x	x	
Cybersecurity Capability Maturity Model	x					x	x	x				
Cyber Power Index	x		x	x	x		x	x	x			
EU Cybersecurity Dashboard	x				x		x	x				x

1.1 Cyber Maturity in the Asia-Pacific Region

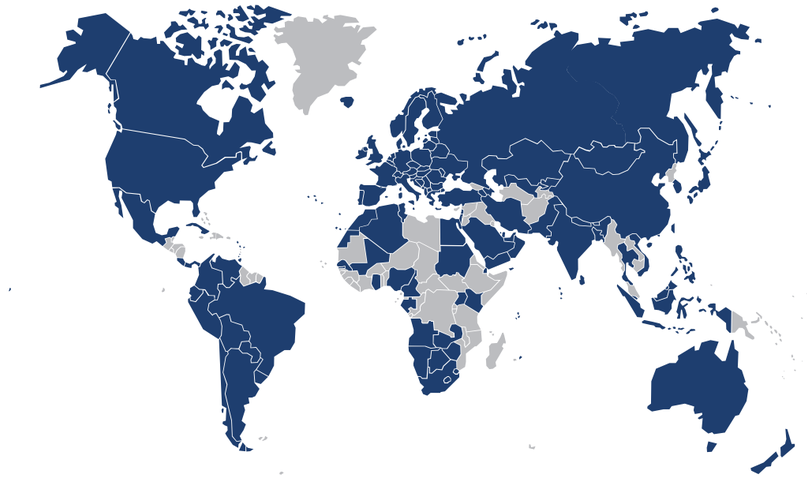


Number of Countries
16
Research Method
Secondary
Rank or Score
Score
Indicators
9

An index developed by the Australian Strategic Policy Institute, which aims to provide information on a nation state's level of cyber maturity. A total of 14 countries in the Asia-Pacific region have been analyzed; with the UK and the US being used as reference points for overall cyber maturity. The index is mainly focused on the policy and organizational aspects of cybersecurity. The methodology proposed uses a 'cyber maturity metric' to assess the various facets of nations' cyber capabilities. A set of nine indicators have been produced and each state's level of cyber maturity has been measured against the benchmark provided with each indicator. The publication includes an overall ranking of cyber maturity for each state within the region, as well as an individual score and short profile. A color coded reference base allows for a quick assessment of cyber maturity for each state. The publication is expected to have further iterations.

The publication is classed as an index since it has indicators, a scoring and a ranking mechanisms. The color-coded reference base is a neat addition. The individual country profiles are helpful and provide a snapshot of national activities. The focus is primarily on organizational structures, legislation, international cooperation, CERTs, and military capabilities. However, it is only a regional index based on open source and publicly available information, and could benefit from a survey based data collection exercise.

1.2 Cyber Readiness Index 2.0.

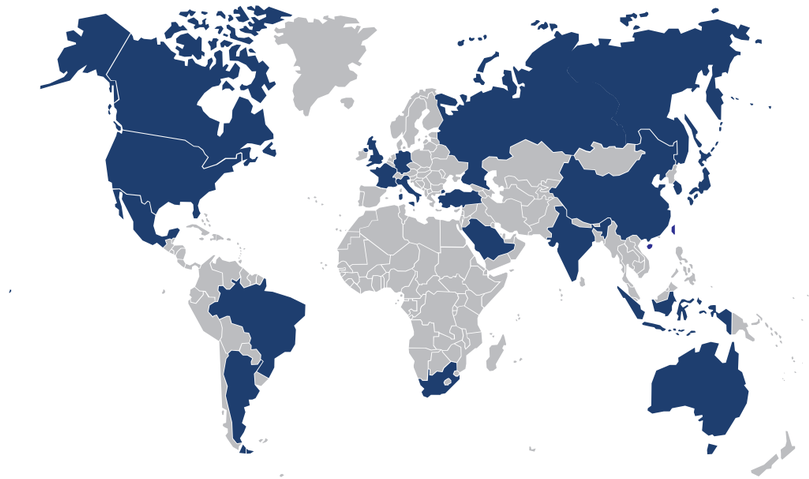


Number of Countries
125
Research Method
Primary & Secondary
Rank or Score
Score
Indicators
7

The index is developed by the Potomac Institute for Policy Studies. The publication is focused on evaluating nation state's cyber maturity as well as their overall commitment to cyber issues. A total of 125 countries have been selected. The publication is mainly focused on policy and economic aspects of cybersecurity and includes fact-based assessments of country's cyber readiness. The index uses a set of seven indicators. The publication is expected to be updated periodically.

The publication has a broad geographic range, and touches upon similar pillars as those enshrined by the ITU's Global Cybersecurity Agenda. Each country has a scoring, and the addition of military capabilities goes beyond that qualified by the ITU GCI. However, it does not offer any ranking, despite a scoring mechanism.

1.3 Cyber Power Index

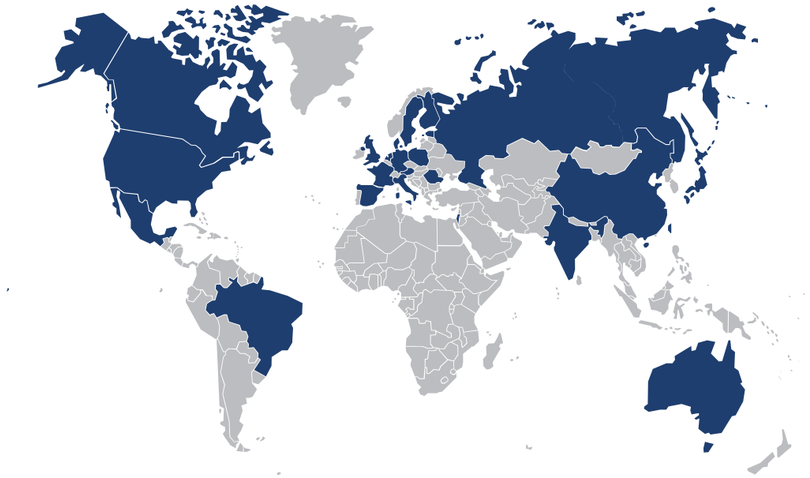


Number of Countries
19
Research Method
Secondary
Rank or Score
Rank & Score
Indicators
39

An index developed jointly by the Economist's Intelligence Unit and Booz Allen Hamilton. The publication is focused on policy, organizational and technical aspects of cybersecurity. The publication includes 39 indicators and sub-indicators grouped into four categories: legal and regulatory framework, economic and social context, technology infrastructure, and industry application. The aim of the publication is to provide a measurement tool for attributes of cybersecurity. The publication covers the 20 countries which are part of the G20. The publication provides scoring and ranking for cyber power of countries under analysis.

The index includes a scoring and ranking mechanism of countries, and focuses primarily on the technical aspects and on industry application. The sub-indicators are weighted according to two different sets. The default weighting is one defined by expert members of a peer panel convened in May 2011. The second weighting option (neutral weighting) assumes equal importance of all indicators. The indicators and categories are modeled according to scores of 0 to 100, where 0 represents the least cyber power and 100 the greatest. The overall score is the result of a normalized score averaged for each indicator. The data for the scoring is gathered from various sources including the UN and other specialized agencies, the WEF, JiWire, OECD, Netcraft, the Economist, and the World Bank. However, it is not a global index and the geographic range is limited to G20 countries.

1.4 Cybersecurity: The Vexed Question of Global Rules

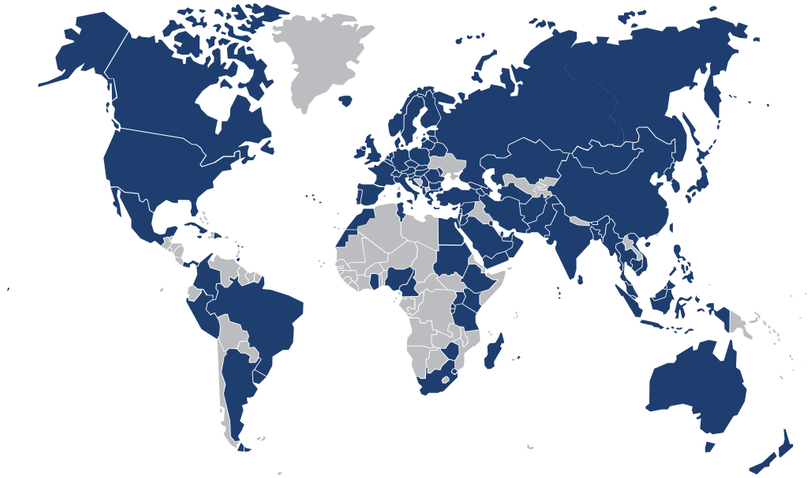


Number of Countries
23
Research Method
Primary
Rank or Score
Score
Indicators
10

A publication developed by the Security and Defense Agenda and McAfee (now Intel Security). The publication offers an overview of the current issues relating to cybersecurity, threat trends and campaigns, cyber defense strategies, debates about rules and regulations to govern cyberspace, and a stress tests of countries' cyber capabilities. The stress tests include 23 country profiles as well as individual scoring developed on the basis of a set of 10 indicators. It is worth mentioning that the publication is based on a survey of 250 leading authorities in the field of cybersecurity. The scoring is based out of 5 stars. The methodology used for rating various countries' state of cyber-readiness is that developed by Robert Lentz, President of Cyber Security Strategies and former Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance. His Cyber Security Maturity Model is a five-step roadmap for reaching resilience, the ultimate goal for governments and businesses that want to effectively operate throughout a sophisticated cyber-attack.

The country stress test is also complemented by policy recommendations and an overview of strategies. The broad group of experts surveyed adds weight to the publication. However, it is limited in geographic range.

1.5 The Cyber Index: International Security Trends and Realities

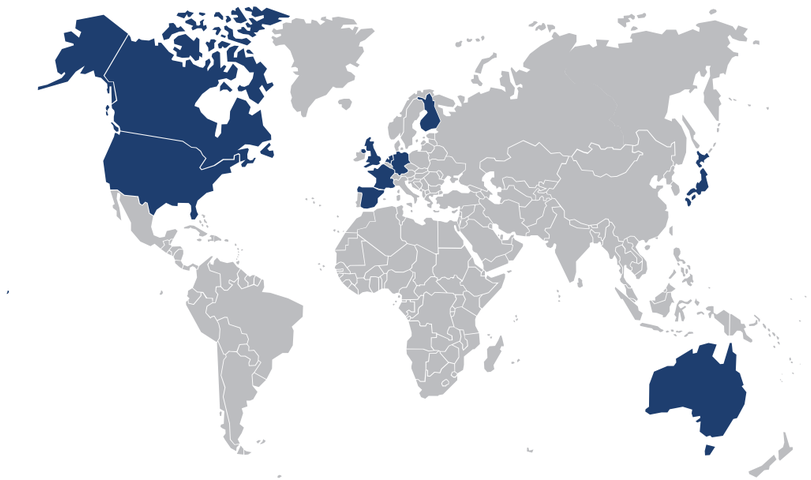


Number of Countries
114
Research Method
Secondary
Rank or Score
None
Indicators
None

A fact-based study of cyber security efforts at an international, regional and national level, developed by United Nations Institute for Disarmament Research. The aim of the publication is to clarify different approaches connected to cybersecurity. The publication is mainly focused on the policy aspect of cybersecurity and includes fact-based assessments of policies or organizations addressing cybersecurity in 114 countries. It also includes information on activities of regional and international organizations in this field. What singles out the publication is the division between countries with a civilian versus military approach to cybersecurity.

The publication has a broad geographic range, detailed country profiles and a good overview of military engagement. The publication uses only open source information and lacks reference to cybersecurity regulation, technical measures (standards, certification), capacity building. Finally, it does not score or rank countries.

1.6 Cybersecurity Policy Making at a Turning Point

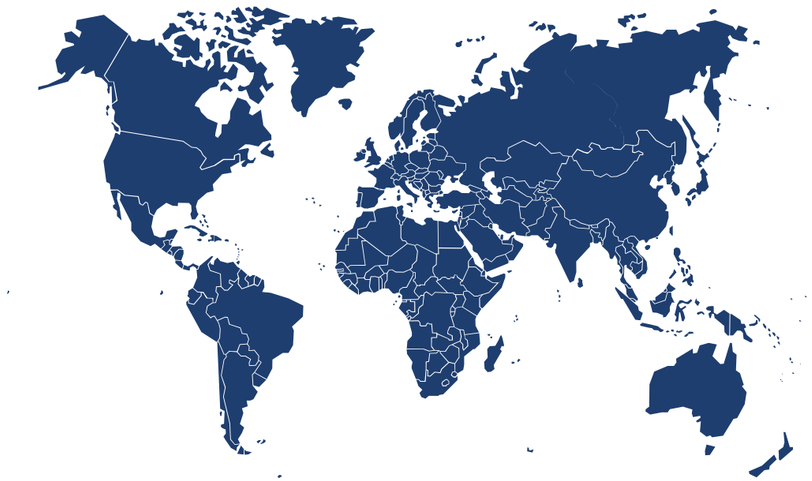


Number of Countries
10
Research Method
Primary & Secondary
Rank or Score
None
Indicators
10

A publication developed by the Organization for Economic Cooperation and Development. The publication analyzes cybersecurity strategies in 10 countries, and provides information on commonalities and differences between them. The publication is based on a questionnaire, filled out by the volunteer countries and supplemented with relevant material. The publication is mainly focused on policy and organizational aspects of cybersecurity. It is worth mentioning that the publication also provides an overview of initiatives undertaken by intergovernmental organizations.

The publication provides a broad overview of strategies, and touches upon all ITU GCA pillars. It further adds a useful overview of intergovernmental organization's initiatives. It does not provide score or ranking and is limited in geographic range.

1.7 Global Cybersecurity Index



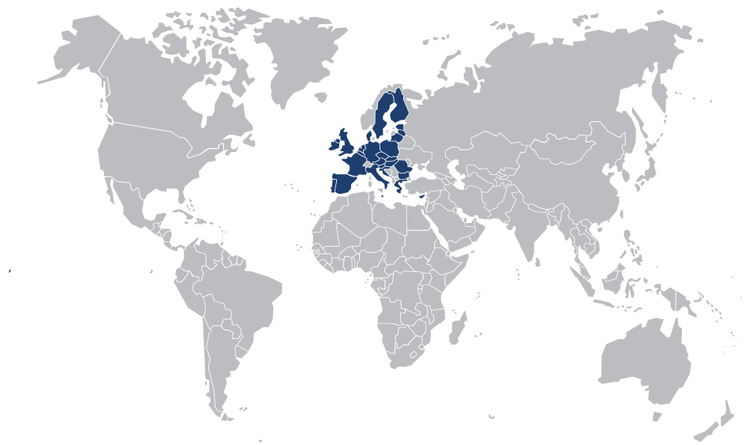
Number of Countries
193
Research Method
Primary & Secondary
Rank or Score
Rank & Score
Indicators
17

An index developed by cooperative effort between ABI Research and the International Telecommunication Union, which aims to provide insight into the cybersecurity engagement of sovereign nation states. Rooted in the ITU's Global Cybersecurity Agenda (GCA), the GCI looks at the level of commitment in five areas: legal measures, technical measures, organizational measures, capacity building, and cooperation. The result is a country-level index and global ranking of cybersecurity readiness. A total number of 194 countries have been analyzed, 104 of which were a subject of both primary and secondary research and 90 only a subject of secondary research. The publication includes an overall ranking, as well as six regional rankings and an individual score for each country. The publication will have further iterations.

The publication is classed as an index since it has indicators, a scoring and a ranking mechanisms. The main advantage of this publication is its global character (the only publication with such broad geographic range). It is based on both survey among ITU Member States and open sourced material. It is worth noting that the publication focuses on five broad cybersecurity application areas with 17 indicators.

However, it is only focused on policy and organizational aspects of cybersecurity and lacks thorough reference to technology.

1.8 EU Cybersecurity Dashboard



Number of Countries
28
Research Method
Secondary
Rank or Score
None
Indicators
25

The Dashboard is a publication developed by BSA, The Software Alliance. The publication is focused on policy and organizational aspects of cybersecurity, with strong reference to legal foundations as well as cooperation between public and private sector. The publication includes 25 criteria across 5 themes, namely: legal foundations for cybersecurity, operational entities, public private partnership, sector-specific cybersecurity plans, and education. The publication covers the 28 European Union Member States. The aim of this cybersecurity dashboard is to provide a reference base which allows the evaluation of country's policies in terms of cybersecurity against 25 criteria and the cybersecurity stance compared to the other EU Member States.

This publication was developed based on publicly available information with no targeted interviews conducted. The methodology of the publication is based on 25 indicators and each indicator is given one of four statuses: Yes, No, Partial, and N/A. The publication does not offer scoring nor ranking mechanisms.

What is interesting about this publication is a graphic reference base which allows for a quick evaluation of countries' cybersecurity stance. The individual country profiles are helpful and provide a snapshot of national activities. The focus is primarily on policy, legal and organizational aspects of cybersecurity with strong reference to public private partnerships. However, it is limited in geographic range to EU countries and could strongly benefit from a survey based data collection exercise.

2. INDICES FOR ASSESSING ORGANIZATIONS

Indices for assessing organizations are slightly different from those outlined above. Primarily, they seek to offer a benchmark or guidelines against which an organization can measure its own level of cybersecurity development or capacity, without necessarily offering a comparative with other organizations. These types of indices are also known as maturity models and offer baselines for organizations, and sometimes even states, to start the process of self-evaluation.

2.1. 2014 Information Risk Maturity Index

An index developed jointly by PWC and Iron Mountain. The scope of the publication is to determine the maturity of information security by businesses. The index includes a set of 34 measures, grouped into four categories: strategy, people, communications, and security. The measures have been developed to foster the management and protection of a company's information assets. The aim of the index is to exhibit the extent to which the above mentioned measures are being implemented and monitored at the enterprise level. As such it is an index that enterprises can use to evaluate themselves. The index offers four levels of information risk maturity: unprepared for risk, risk aware, approaching maturity, and equipped for risk. The index is mainly focused on the organizational aspect of cybersecurity. The publication offers some scoring results on information risk maturity and provides distribution of the results by region (Europe and North America only) and size of the company.

2.2. Risk and Responsibility in a Hyperconnected World

A publication developed jointly by the World Economic Forum and McKinsey & Company. The aim of the publication is to assess the potential impact of cyberattacks as well as readiness to response and present key areas where global leaders across the spectrum of private and public sectors and civil society can collectively explore to increase cyber resilience. The publication also identifies key action areas that should be explored in terms of increasing cyber resilience. Those areas are grouped into four categories: institutional readiness, public and international policy, community, systemic. The publication is based on interviews with industry leaders as well as surveys undertaken among multiple sector firms.

2.3. Cyber Operations Maturity Framework

A publication developed by Booz Allen Hamilton. The publication presents the company's approach to cyber operations which includes an Operational Model for organizations. This model integrates four functions: Anticipation, Awareness, Action, and After-Action. The publication provides five maturity levels in eleven key operational areas. The publication is mainly focused on operational aspect of cybersecurity.

2.4. Cybersecurity Capability Maturity Model

A publication developed by the University of Oxford's Global Cyber Security Capacity Centre. The aim of the model is the creation of a universally applicable cybersecurity maturity model. The publication defines five capacity dimensions related to cybersecurity, namely: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory framework; and organizations, technologies, and standards. The publication identifies set of 49 indicators depicting varying levels of cybersecurity capacity development. The publication is mainly focused on policy and organizational aspects of cybersecurity.

3. INDICES FOR ASSESSING THREATS

Indices for assessing threats are the third group of indices determined in this study. First and foremost, they evaluate the level of risk attributed to cyberattacks, incidents, security events, and vulnerabilities, among other threat scenarios. They do not evaluate organizations or nation states, but simply provide a measurement of the threat landscape. This information can primarily be used for intelligence and awareness purposes. The indices are often developed by individual academics and security practitioners, and private sector organizations.

3.1. Cybersecurity Intelligence Index

The index is developed by IBM's Managed Security Services. The publication includes an overview of cybersecurity threats based on cyberattack event data gathered by the company. The data is gathered by monitoring client security devices and analysis from IBM's security operations centers. The publication provides a broad overview of technical challenges, case studies, and best cybersecurity practices in private sector. The Index does not score or rank organizations or countries, nor does it include any specific indicators or formula for the calculation of an index. Rather it provides the overall number of security events, attacks and incidents in the given year, as well as distribution by industries, category of incidents and category of attackers. The publication is expected to be updated periodically.

3.2. Index of Cybersecurity

This index is an individual effort developed by Dan Geer and Mukul Pareek, and is focused on the technical aspect of cybersecurity. It is an opinion-based measure of perceived risk to information infrastructures from a wide range of cybersecurity threats. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite. The publication gathers the views of information security professionals on the most current and most interesting threats to governmental, corporate, and industrial information infrastructure through a monthly survey. The index is based on a variation of the diffusion index methodology. The publication is updated on a monthly basis. The aggregate index value is updated on a public website each month. However, detailed statistics and individual sub-indices are shared only with respondents in a separate report.

3.3. Cybersecurity Index

An index developed by Dell Secure Works. The aim of the publication is to notify customers about threats and malicious activities which may require implementing protective measures. The publication uses a 4 level scoring system of overall network cybersecurity status which in a simple and readable manner informs customers about the current level of overall cybersecurity threat. The index is not numerical but simply color-coded based on the following four cybersecurity levels: Guarded, Elevated, High, and Critical. The threats are determined by a panel of experts at the Dell SecureWorks Counter Threat Unit Research Team and based on information such as the release of security updates by companies such as Microsoft and Adobe. The publication is focused on technical aspect of cybersecurity and is evaluated on a day-to-day basis.

3.4. The Gibson Index

The index is an individual effort developed by Kevin Boyd. The publication is mainly focused on the technical aspect of cybersecurity. The index offers a way to rank the level of severity of cyberattacks on a scale from 0 to 7, with 0 being the least disruptive and 7 the most disruptive. The levels are determined through definitions and examples of events in each level. The document is still an early draft and currently does not provide scoring for any types of events. The publication is expected to be updated periodically. The Gibson Index was shut down by the author in June 2015.

4. Conclusions

The above overviews only provide a snapshot of some of the more relevant cybersecurity publications. However, there are various other indices and models which are equally important, though different in scope. They are still worth mentioning as they are important contributions to the global knowledge base of cybersecurity related research efforts.

The Cybercrime Repository is a publication developed by United Nations Office of Drugs and Crime. The publication provides overview of cybercrime legislation around the world. It is basically a digital repository of data on cybercrime legislation, cybercrime case law and practices in preventing and combating cybercrime. The aim is to provide a tool which will facilitate the evaluation of needs and capabilities of criminal justice systems as well as providing coordinated technical assistance.

The publication has a broad geographic range and touches mainly upon legal aspects of cybersecurity. The publication does not offer any ranking nor scoring mechanism and for that reasons is not really an index or a model. Nevertheless, the publication touches upon an important aspect of cybersecurity, which is the law, and covers most UN Member States, providing a profound overview of legislative and strategic activities. For this reason it deserves recognition in this paper.

Slightly less extensive but still relevant are other efforts, such as the work done by the Data Security Council of India (Public Private Partnerships (PPPs) models in cybersecurity - Indian perspective) and Jamaica University (Promoting effective Cybersecurity Management in Developing Economies: The Cybersecurity Capability Maturity Model). Further, a publication by the United Nations Conference on Trade and Development (UNCTAD) entitled The Information Economy Report 2015 includes some relevant information on cybersecurity. Finally, United Nations Interregional Crime and Justice Research Institute (UNICRI) has also published a report on Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level.

There are likely to be many more ongoing research projects in this field, and while this paper does not provide a finite list of all, the aim is to provide a brief overview of some of them in an effort to continue to educate and inform on the value of indices, models and repositories.