# Understanding the Institutional Landscape of Cyber Security

Cecilia Testart

August 2016

**Abstract**

The decentralized architecture of the Internet, which has been key to its development and worldwide deployment, is making it challenging to secure Internet user experience. Many organizations claim to be playing a role in improving Internet security. If anything, the space of security-related institutions seems on first inspection to be over-populated, yet poor security persists. This work proposes a framework to understand the role different institutions play in cyber security. The analysis gives insights into the broad institutional ecosystem of public, private and international actors, and the varied nature of these institutions, their interests, incentives, and contributions to cyber security from hardware, software, protocols, standards and regulation. Based on natural language clustering algorithms, this framework classifies institutions along five dimensions: the aspect of cyber security the institution covers, the industry and activity sector of the institution, whether it is part of a specific jurisdiction, specific institution's characteristics such as its working mode or primary focus, and the institution governance type. This work is based on a dataset that was developed including approximately 120 institutions playing a role in cyber security. Using this framework, it is possible to better understand the nature of the large number of organizations currently shaping cyber security, the relationship between them, areas of competing and overlapping institutional interest, and the overall structure of institutional responses to cyber security.

## 1 Introduction

Since the inception of the Internet, its architects and researchers have been trying to increase the overall level of security, developing tools such as encryption and authentication protocols. The decentralized architecture of the Internet has been key to its development, but its worldwide deployment is making it more challenging to secure the Internet user experience. Although most providers work to secure their products and services, these efforts are fragmented, and systemic vulnerabilities remain to be exploited to harm Internet users when they use online services or connect devices. In fact, there are many organizations that claim to be playing a role in improving Internet security, with different origins, specializations and modes of operation. If anything, the space of security-related institutions seems on first inspection to be over-populated, yet poor security persists.

A framework based on different institutional characteristics is proposed to understand the role different institutions play in cyber security. This analysis gives insights into the broad institutional ecosystem of public, private and international actors, and the varied nature of these institutions, their interests, incentives, and contributions to cyber security, from hardware, software, protocols, standards and regulation. The framework classifies institutions along five dimensions: the aspect of cyber security the institution covers, the industry and activity sector of the institution, whether it is part of a specific jurisdiction, how the institution carries out its work, and the institution governance type.

This work is based on dataset of approximately 120 institutions that play a role with respect to cybersecurity. To create the dataset, institutions listed in cyber security national strategies and cyber security policy literature were considered. Additionally, institutions that were involved in cyber security discussion during the Internet Governance Forum of 2014 were also examined and considered for the dataset, capturing many more private sector institutions that are actively participating in cyber security policy-making and relevant for internet user's security.

Natural language clustering algorithms are used as a semi-supervised learning technique to extract structure from the transcribed discourse describing institutions, their activities and their relationship with cyber security. The aspects of cybersecurity covered by the institutions in the dataset include cybercrime, cyber defense, computer security, network security, security standards and data security. Public sector organizations, international organizations and not-for-profit organizations related to governments are classified as to whether they are associated with the US, the EU, or other parts of the world. Industry sectors include finance, telecommunications, software, hardware and service providers, online services and Internet governance. Specific characteristics of institutions include the working mode of these institutions, such as forum and convening activities, information sharing, and specific committee or working group to address cyber security, and also the primary focus of larger institutions (such as economic development and consumer trust) that are now concerned with cyber security.

Using this framework, it is possible to better understand the nature of the large number of organizations currently shaping cyber security, the relationship between them, the areas of competing and overlapping institutional interest, the areas out of scope of current institutions and the overall structure of institutional responses to cyber security.

This work builds on previous studies that focus on particular sets of institutional responses to cyber security such as the computer emergency response teams (CERTs) development [1], public policy for cyber security [2] and international cooperation and agreements to enhance cyber security [3].

Moreover, in the few last years, international organizations have published documents where they explain the role of different bodies in national strategies and other efforts for cyber security [4, 5, 6]. The different parts of the institutional landscape these texts lay out are used as a starting point of the institutional analysis.

# 2 Methods

The methods to study cyber security institutions had three main steps: (1) building the dataset of institutions shaping internet security, (2) extracting meaningful clusters of institutions from the dataset using semi-supervised learning to build a framework, and (3) analyzing institutions using the framework.

## 2.1 Building the dataset

It was considered that there are two ways in which an institution can *shape* internet security:

1. the institution significantly influences the security of internet users' experience, such as large software and hardware providers;
2. the institution is actively participating in the cyber security ecosystem, such as many private organizations that publish reports based on their own data or organize workshops to discuss particular issues.

Institutions that comply with one or both of these specifications are included in the dataset. Three different sources contributed institution names to the dataset: existing cyber security policy literature, government and international organizations publications, and institutions mentioned in cyber security discussions from Internet Governance Forum transcripts.

After studying previous works and public sector publications, there was still a major gap in terms of private actors that play relevant roles in cyber security. Indeed, most of the Internet infrastructure, hardware and software that enable users' experience are in the hands of private actors. Therefore, it is key to understand companies and not-for-profit organizations' role and involvement in securing the internet. The challenge is to select these private actors.

Scraping entity names in the transcripts from IGF 2014 discussions in portions of the text where keywords related to security were mentioned provided a list of public and private institutions mostly shaping internet security according to the criteria defined at the beginning of this section. More detail about the algorithm used for entity name extraction can be found here [7].

For each institution in the dataset, their webpage and available publications were used to capture the language they use to describe their main activities and activities related to cyber security. The following institution information is included in the dataset:

- The type of organization: is it a governmental, international, not-for-profit, for-profit organization?
- The role of the institution: is it a forum, a provider of software, hardware or services, an operator, etc?
- The relationship to cyber security: what is the organization doing relevant to cyber security?
- The date of creation: date of creation of the main organization behind working and research groups and initiatives in cyber security.

Using the three sources described above, 124 institutions were included in the dataset at the time of writing, with the description of the institutions' activities and role in general and specifically for cyber security. The full list of institutions can be found in Appendix A.

## 2.2 Clustering institutions

Semi-supervised clustering was used to explore the data and discover underlying structures and similarities between institutions in the dataset . After trying different algorithms such as k-means and Suffix Tree Clustering (STC), the Lingo algorithm was selected as its clusters better represented distinctive characteristics of institutions. After assessing the algorithm clusters, institutions' classification in the clusters was reviewed to evaluate if other institutions of the dataset should be associated with the cluster. Chapter 2 in [7] describes in detail the clustering process.

The final list included 28 clusters highlighting specific characteristics of the institutions that were categorized in five dimensions depending on the cluster description: the cyber security aspects institutions were focusing on, the activity sector of the institutions, the geographical region of the institutions, specific characteristics of the institutions mode of operation, and the governance mode of institutions.

### 2.3 Analysis of clusters and institutions using the framework

The clustering results were analyzed by looking at the institutions in different clusters and also studying the relationships between clusters in different dimensions, exploring how institutions in clusters from one dimension are classified in other dimensions.

Additionally, institutions that were not classified in any cluster in some dimension were studied to understand why there is no specific cluster that represents their characteristic, examining in particular categories that are over or under-represented in the different clusters.

Finally, it was considered how institutions that were not in the dataset could be studied and how they fit in the ecosystem using the framework.

## 3 Institutions shaping Cyber Security

Using the procedure described in 2.2 institutions are classified into 28 different clusters corresponding to distinct characteristics of the institutions and their work. The clusters are organized in five dimensions capturing the different topics of the clusters: cyber security aspects, activity sectors, jurisdictions, institutional characteristics and governance types[1]. Figure 1 shows the five dimensions and the clusters in each of them.

The clusters of institutions are based on similarities between institutions' role in general and their approach and work on cyber security, to organize the landscape

[1] In this context, governance refers to the way institutions are themselves governed, not to the governance of the Internet or cyber security.

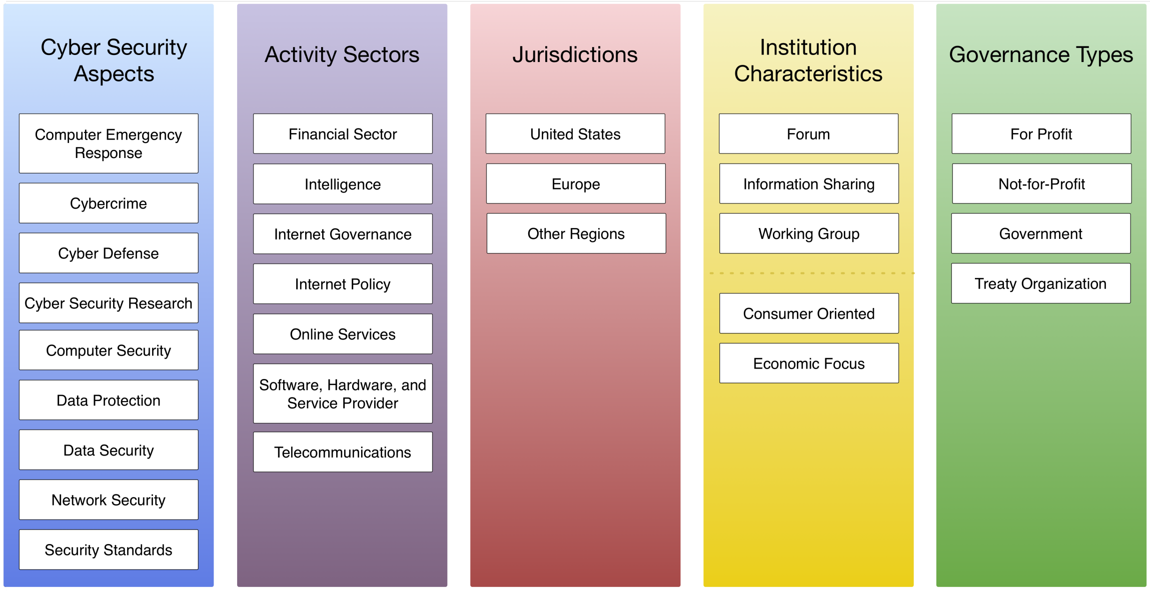

Figure 1: Framework of institution clusters organized by dimensions.

and bring more insight about the role each institution is playing. Chapter 3 in [cite Thesis ] reviews the institutions in each cluster, giving a sense why institutions are classified there.

Except for the governance type dimension, not all 124 institutions are classified in a cluster in each dimension, and except for governance and jurisdiction dimensions where the clusters are mutually exclusive, institutions may be part of two or more clusters within the same dimension.

## 3.1 Establishment of the institutions in the dataset

Although cyber security is a fairly new domain, government institutions that are shaping cyber security policy were created as early as 1789, and have expanded their scope to cover cyber security. However, most institutions in the dataset are relatively young, with over 50% created in or after 1998. Figure 2 depicts the number of institutions in the dataset in place from 1789 to 2015, by type of governance.

The largest increase in the number of institutions comes from the boom of not-for-profit institutions created after the World Wide Web was born in 1989. The second largest growth happened a few years earlier, with the advent of computer and technology companies. And after the year 2000, we can see that many national and

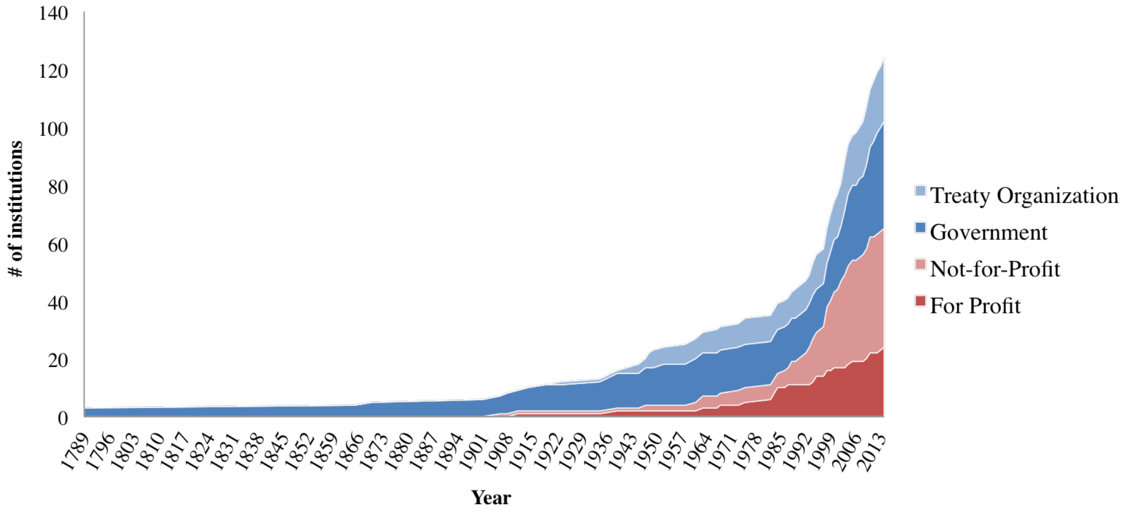

Figure 2: Number of institutions in place per type and per year from 1789 to 2015.

international government organization related to cyber security were created. Indeed, many institutions were created as part of the development of the European Union, and others are the result of the increasing relevance of cyber security for governments around the globe.

# 4 The diverse governance of cyber security institutions

Institutions of the cyber security ecosystem in the dataset have very different governance nature: they can be a not-for-profit organizations, for-profit private companies, international organizations or part of a government.[2] Table 1 has a few samples of institutions in the dataset and their governance type. The full institution list and their governance type is available in Appendix A. Figure 3 gives a general overview of the distribution of the different types of governance across institutions in the dataset.

[2] In this context, the European Union agencies and bodies established by the European Union or the European Council are considered as government organizations and not treaty organizations, unless they are clearly based on a treaty document.

| Institution | Governance |
|---|---|
| IETF : Internet Engineering Task Force | Not-for-profit |
| M3AAWG : Messaging, Malware, Mobile Anti-Abuse Working Group | Not-for-profit |
| DHS : Department of Homeland Security | Government |
| ENISA : European Union Network and Information Security Agency | Government |
| CISCO | For profit |
| Google | For profit |
| OAS : Organization of American States | Treaty Organization |
| IMPACT : International Multilateral Partnership Against Cyber Threats | Treaty Organization |

Table 1: Sample of institutions and governance type.

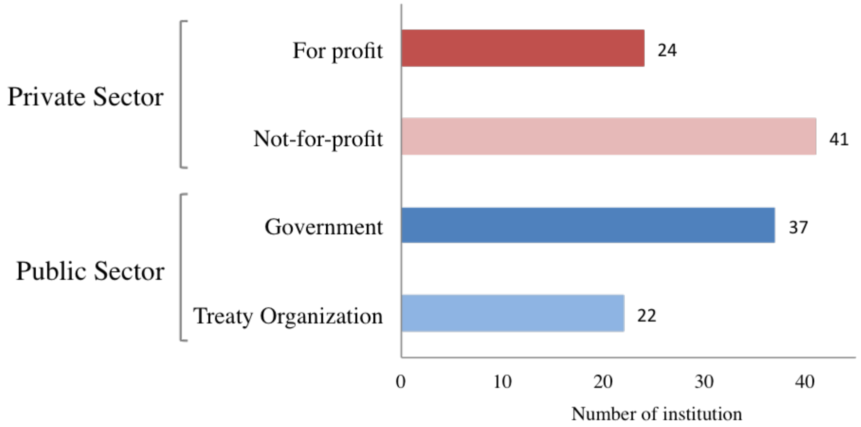

Figure 3: Institution counts per governance type: private sector institutions in red and public sector institutions in blue.

Clusters in the governance type dimension are based on an intrinsic characteristic of the institutions. The four governance types are well represented, with private institutions playing a major role in cyber security. Indeed, more than half the institutions found are private, whether for-profit or not-for-profit organizations.

Within the not-for-profit cluster, institution may play very different roles. For instance, the Internet Engineering Task Force (IETF) is a not-for-profit organization[3] that has been very close to the technichal community since its inception, focused on "making the Internet work better"[cite IETF webpage]. In contrast, there are not-for-profit organizations, specially in Europe, that work very closely with governments

[3] The IETF is housed in the Internet Society (ISOC) a not-for profit organization.

and act almost as government agencies. For example, the European Committee for Electrotechnical Standardization CENELEC is a not-for-profit organization that was designated as a European Standard Organization by the European Commission and works closely with other European standardization bodies to support the development of a single European market, covering cyber security standards.

# 5 Distinct cyber security activities

This section focuses on the clusters in the cyber security aspect dimension, which groups clusters that capture the areas of cyber security the institutions in the dataset are focusing on: Computer Emergency Response, Computer Security, Cybercrime, Cyber Defense, Cyber Security Research, Data Protection, Data Security, Network Security and Security Standards. Institutions are associated with the specific topic of the cluster by what the institution is doing related to cyber security. Table 2 shows a sample of institutions in the different clusters and their governance.

## 5.1 Clusters in the cyber security aspect dimension

There are nine clusters in the cyber security aspect dimension and 89 institutions in the dataset are classified into at least one of these clusters. Figure 4 shows the proportional size of each of the clusters in the cyber security dimension. The largest cluster is network security with 27 institutions, followed by cybercrime with 19 and security standards with 13. The smallest clusters are cyber defense, cyber security research and computer security, with four, five and six institutions of the dataset respectively.

The composition of the clusters in this dimension, in terms of types and number of institutions, is varied. For example, the network security cluster is large, with a mix of institutions from the private sector and also government agencies that are working to secure networks. In contrast, the cyber defense cluster is small and uniform, with all institutions coming from the public sector. Similarly, the cyber crime cluster is dominated by the public sector, with many government agencies and treaty organizations of the dataset collaborating and cooperating in fighting cyber crime at national and international levels. Then, the security standard cluster has mainly not-for-profit organizations and a few government agencies that are developing cyber security standards for different products and markets.

The data protection and data security clusters are interesting because although both cluster focus on information security, they have different motivations and objec-

| Institution | Cluster | Governance |
|---|---|---|
| FIRST : Forum for Incident Response and Security Teams | Computer Emergency Response | Not-for-profit |
| AP-CERT : Asia Pacific Computer Emergency Response Team | Computer Emergency Response | Treaty Organization |
| Microsoft Corporation | Computer Security | For profit |
| Symantec | Computer Security | For profit |
| DHS : Department of Homeland Security | Cybercrime | Government |
| EEAS : European External Action Service | Cybercrime | Government |
| US Cyber Command | Cyber Defense | Government |
| NATO : North Atlantic Treaty Organization | Cyber Defense | Treaty Organization |
| EC JRC : European Commission Joint Research Center | Cyber Security Research | Not-for-profit |
| CERT/CC : CERT Coordination Center | Cyber Security Research | Not-for-profit |
| FTC : Federal Trade Commission | Data Protection | Government |
| LAP : London Action Plan | Data Protection | Not-for-profit |
| ODCA : The Open Data Center Alliance | Data Security | Not-for-profit |
| Symantec | Data Security | For profit |
| M3AAWG : Messaging, Malware, Mobile Anti-Abuse Working Group | Network Security | Not-for-profit |
| Verizon : Verizon Communications | Network Security | For profit |
| NIST : National Institute of Standards and Technology | Security Standards | Government |
| ISO : International Organization for Standardization | Security Standards | Not-for-profit |

Table 2: Sample of institutions in clusters of the cyber security aspect dimension.

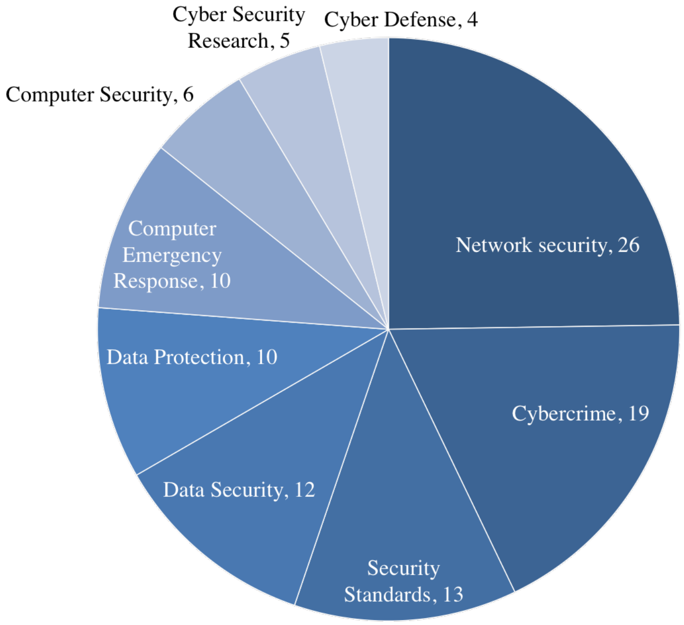

Figure 4: Distribution of institutions in the cyber security aspect dimension: number of institutions in each cluster.

tives. The data protection clusters is composed of institutions that view information security from the end user perspective and the minimum level of data protection users should have, whereas institutions in the data security cluster either develop technologies to secure data or have the responsibility of securing data. Therefore, most for-profit institutions are in the data security cluster, as they focus on the technology. However, there is an information security company in the dataset that is in both clusters. Gemalto[4] is one of the first companies to publicly disclose that its products are compliant with the data protection requirements of the new EU General Data Protection Regulation, which was approved by the legislative institutions of the European Union on April 14th, 2016, although the new rules will be applicable in 2018 [8].

Because of a methodology constraint, there is no for-profit private institution in the computer emergency response. Indeed, although most large companies and organizations relying heavily on IT have a Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT), in the dataset were included only the ones playing a larger role and shaping the ecosystem mainly by their role within the CERT/CSIRT community.These institutions turned out to be

[4] Gemalto recently acquired the US-based information company SafeNet.

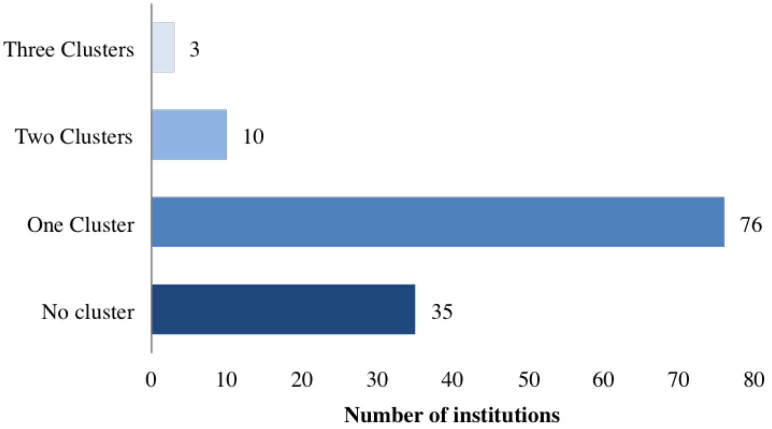

Figure 5: Number of institutions that are in zero, one, two and three clusters of the cyber security aspect dimension

not-for-profit, government or international organizations.

For the computer security and cyber security research cluster, the methodology to build the dataset captured specific groups of institutions. The computer security cluster is composed of large technology companies that are either manufacturers of computers or processors such as Microsoft, Hewlett Packard and Intel, or security software companies such as Symantec and McAfee (now Intel Security Group - McAfee), and there are no governmental institutions in this cluster. In contrast, only not-for-profit organizations comprise the cyber security research cluster. This is probably not representative of the governmental efforts in cyber security research and computer security. However, other methods should be used to capture this.

## 5.2 Relationship between clusters in the cyber security aspect dimension

Over 50% of institutions in the dataset are specific enough in their relationship and activites with respect to cyber security to focus on only one cyber security aspect. In fact, as Figure 5 shows, 76 of the 124 institutions in the dataset are classified in one cluster in the cyber security dimension, 10 institutions are in two clusters, and only three institutions are in three clusters.

Depending on the governance of institutions, there are different reasons why an institution in the dataset focuses on more than one cyber security ascpect. The public sector institutions that are in more than one cluster have a mandate that covers the different topics of the cluster they are in. For instance, the Korean Internet and Security Agency is in charge of data security of Korean government networks and critical infrastructure and at the same time it develops the personal data protection framework. Similarly, the US Department of Defense (DoD) is responsible for the security of its networks and the US cyber defense posture. The not-for-profit organizations that are in multiple clusters typically extended their scope probably as a result of their leadership. As an example, the Latin American Top-Level Domain (LacTLD) managers association provides network security training for top-level domain managers in the region and also collaborates with local law enforcement agencies in cybercrime and computer forensic. The CERT Coordination Center (CERT/CC), the first Computer Emergency Response Team that was created, is now also doing cyber security research, collaborating with many US government agencies. Finally, the companies that are in multiple cyber security aspect clusters are mainly security software companies such as Symantec and Intel Security Group - McAfee that cover several topics including computer, network and data security.

To give a visual idea of the cluster relationships in the cyber security aspect dimension, in Figure 6 links between institution and the clusters they are in are represented. Red links emphasize the links of institutions that are in two or more clusters.

Additionally, there are 34 institutions in the dataset that are not classified in any cluster of the cyber security aspect dimension. None of these institutions focus on any of the aspects captured by the clusters. Indeed, the six companies not listed in clusters in this dimension offer products and services whose security has an impact on users' experience but these companies do not focus on any particular aspect of cyber security. For instance, many aspects of security represented by the clusters are relevant for Google, Facebook and Paypal services and therefore they do not concentrate on only a few of those topics. Similarly, the international institutions not listed in this cluster address cyber security as one topic of their internet policy and regulation activity. And most of the government institutions not classified have a high-level responsibility related to the internet ecosystem and address cyber security in general. For example, the US Department of State coordinates the global diplomatic engagement on cyber issues of the US, the Colombian Communications Regulation Commission is in charge of all matter related to communications, including the internet in its country, and the Organization for Economic Co-operation and Development (OECD) studies and supports its member countries' policy making in all aspects of cyber security. However, there are government institutions and not-for-profit organizations that address other topics related to cyber security aspects that do not constitute a cluster in the framework because only one or two institutions in the dataset at the time of writing focused on those topics. For instance, the US

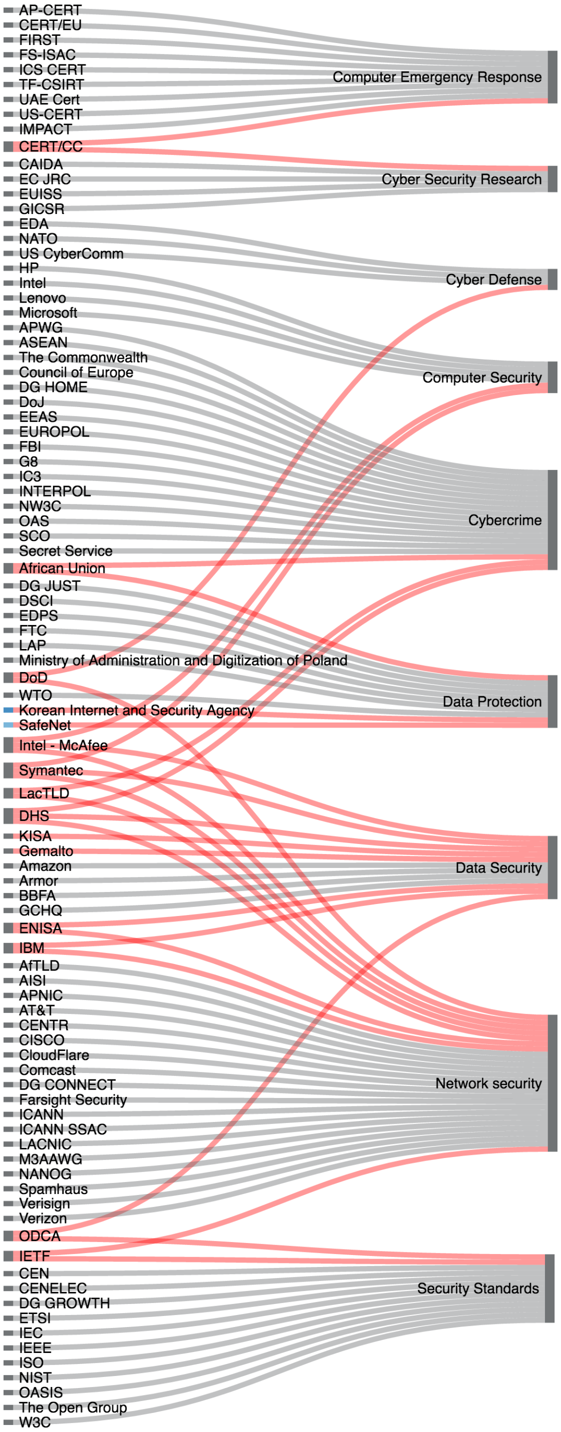

Figure 6: Institutions in cyber security dimension clusters. Red links indicate institutions in more than one cluster.

National Security Agency is in charge of US national security in cyberspace, covering most if not all cyber security aspects. And the not-for-profit National Cyber Security Alliance and ConnectSafely.org work to increase consumer awareness of cyber security threats and foster preventive practices in many cyber security areas.

## 5.3 Governance types in cyber security aspect clusters

Studying in more detail the governance of institutions in the different cyber security aspects sheds light on how different priorities are according to institution governance types. Figure 7 shows the number of institutions of each type in the cyber security aspect cluster. The graphs reveal that private sector institutions (for-profit and not-for-profit) generally focus on narrowed aspects of cyber security in comparison to the public sector (including government agencies and international organizations), as there are very few private sector institutions that cannot be classified into these clusters ('Not specified' category in figure 7 (a) and (b)).

Moreover, for-profit institutions concentrate mainly on a few areas of cyber security: network, computer, and data security. Network security is the largest cluster among private sector institutions but there are only a few government institutions in the cluster and no treaty organizations. This is in line with the fact that most of the Internet infrastructure is in the hands of private institutions.

Figure 7 (b) also illustrates the relevant role not-for-profit institutions play in cyber security. Indeed, in the dataset, there are not-for-profit organization in all aspect clusters except computer security and cyber defense.

Government institutions are also well distributed across all clusters of the cyber security aspect dimension (Figure 7 (c)). They are in all clusters except computer security and cyber security research. However, the fact that government institutions do not directly cover those areas does not mean that governments are not working on those areas, as governments fund research of other institutions.

Finally, treaty organizations concentrate in the cybercrime cluster mostly, and in a lesser extent in the data protection cluster.

## 5.4 The many activity sectors of institutions in cyber security aspect clusters

Analyzing the activity sector of institutions in the cyber security clusters reveals that most institutions in cyber security clusters do not have a specific activity sector. In

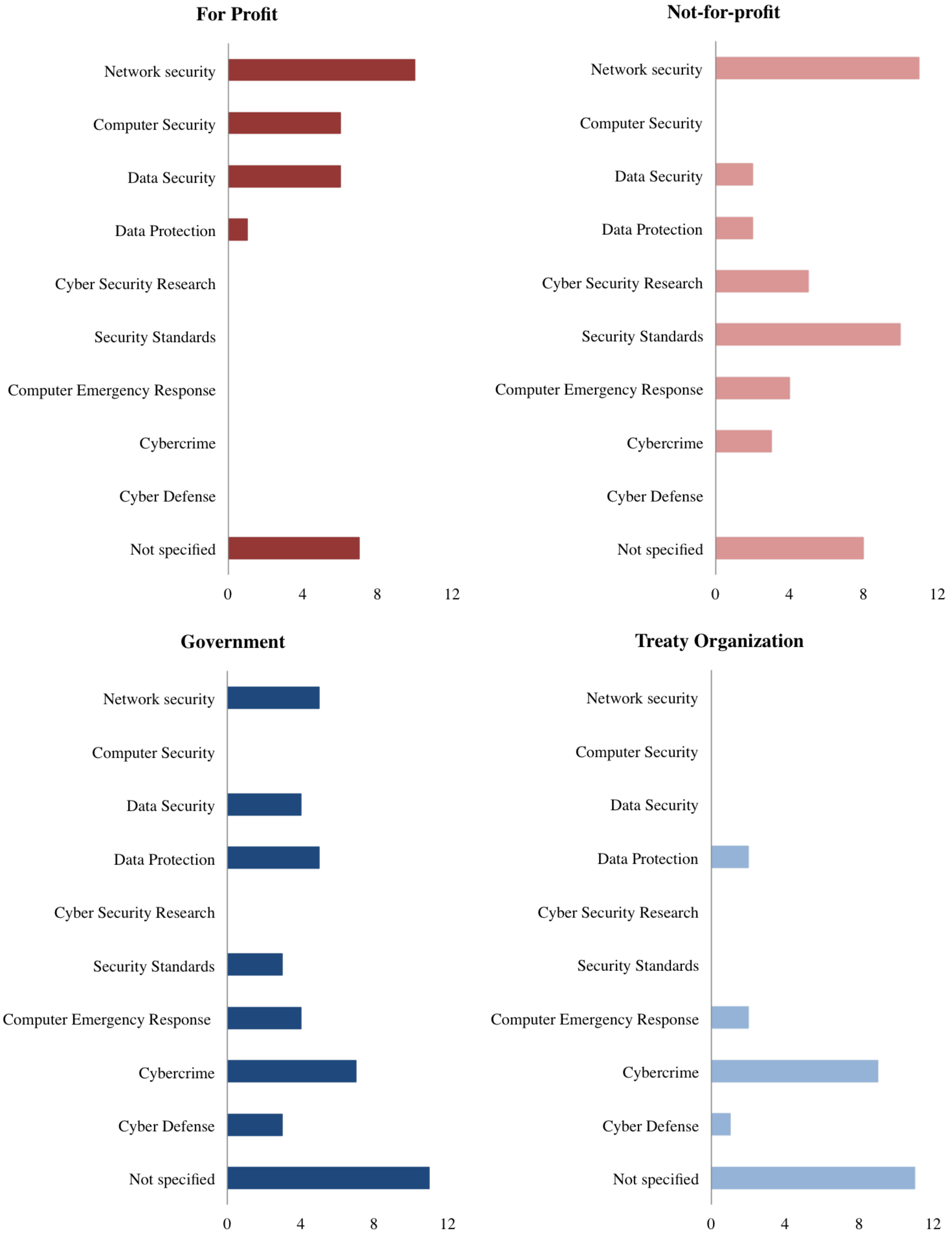

Figure 7: Distribution of (a) for profit, (b) not-for-profit, (c) government, and (d) treaty institutions in cyber security aspect clusters.

fact, only 27 of the 90 institutions in this dimension are also in a cluster in the activity sector dimension. Furthermore, no institution from the dataset in the cyber defense and cyber security research is in an activity cluster, and similarly, most institutions in the computer emergency response, cybercrime and data protection clusters do not have a specific activity sector. Although specific areas of cyber security, these topics are not specific to particular industries and activities at the national and international levels and therefore institutions concentrating on them do not necessarily come from a particular activity sector.

In contrast, there are many institutions in the computer, data and network security clusters that are also in the software, hardware and service provider cluster. These are the large hardware, software and information security companies, such as Microsoft and Symantec, that are leading the effort to secure their products and offer security solutions to users.

Moreover, institutions in the network security cluster come from many different activity sectors. Institutions in the Internet governance, internet policy, software hardware and services provider and telecommunications clusters are working on network security. Indeed, institutions from all these different sectors make the Internet work and have a significant impact on the overall security of the network.

## 5.5 Jurisdiction of institutions in cyber security aspect clusters

Almost half of the institutions in the cyber security clusters have a defined jurisdiction or geographic zone for their work. Computer security is the only cluster where there is no institution in the dataset that is also in a jurisdiction cluster. Naturally, tech companies in the computer security cluster are not attached to a particular jurisdiction and their products are available globally.

In agreement with the findings in section 5.3, most institutions in the cybercrime cluster have a specific jurisdiction as they are mostly government or international institutions, with the US and Europe having many different institutions participating in the cybercrime efforts.

In addition, 10 of the 26 institutions from the dataset working on network security have a defined jurisdiction. Indeed, these institutions are either the ones in charge of network security for their government, such as the European Union Network and Information Security Agency, or are regional not-for-profit organizations related to Internet resources, namely domain names and addresses, such as Asia-Pacific Network Information Centre, which distributes Internet Protocol (IP) addresses in the Asia-

Pacific region.

Finally, in the security standards cluster, four of the 13 institutions from the dataset classified in this cluster are from Europe. These four institutions collaborate in the development of standards for the European Union single market in accordance with the EU cyber strategy.

## 5.6 Other institutional characteristics of institutions

In most of cyber security aspect clusters, there is one or more *forum* institutions, only the computer security, cyber defense and cyber security research clusters do not have one. These forums are either not-for-profit institutions that have emerged from a need between different actors to share experience and best practices, enhance trust and collaboration, such as the Forum for Incident Response and Security Teams (FIRST), or they are treaty organizations, such as the Organization of American States, that have used their institutional background to set common ground rules between member states in topics including cybercrime and critical infrastructure protection.

In addition, there are four forums in the security standard cluster. Three of these forums concentrate on information standards for interoperability and convergence, although with somewhat different interests: the Open Group focuses on technology integration, the Open Data Center Alliance focuses on interoperable solutions for cloud computing, and the Organization for the Advancement of Structured Information Standards focuses on open standards.

In computer emergency response, most institutions have a mission in *information sharing* as a significant part of their objective is to consolidate and distribute information about incidents and responses with the different organizational units of the institution they are housed in. Nonetheless, there are information sharing institutions in other clusters such as the coalition for a global response to cybercrime Anti-Phishing Working Group, which fosters information sharing between industry, government, law enforcement agencies and non-governmental organizations.

In the cybercrime and security standard clusters, there are institutions that have an *economic focus* as their main objective is closely related to economic development. As cybercrime and security standard relevance for economic development increased, these institutions started working on these cyber security aspects. Similarly, other institutions in these clusters have a more general objective and create a *working group* to focus on these aspects, such as the International Organization for Standardization (ISO), which has created many working groups for different cyber security standards such as the information security suite ISO/IEC 27000.

## 5.7 Missing institutions

The dataset of institutions built is of course still missing institutions working on cyber security and shaping cyber security policy. The methodology used to find institutions makes some institutions more visible than others. Many institutions come from IGF discussions, where attendees and topics are influenced by global issues affecting the Internet ecosystem in general. As such, if the same procedure was applied to capture the institutions in cyber security discussions in such a conference now, probably Apple would be part of the list, because of all the exposure related to the encryption contention with the Federal Bureau of Investigation (FBI) in the US[5]. Furthermore, Apple would perfectly fit in the framework: it would be in the data security and software, hardware and services provider clusters.

Additionally, there are institutions working on some cyber security aspects that are unlikely to be noticed with the method used to buid the dataset, and other ways of collecting data would be more suitable. For instance, studying research funds from different government agencies would allow to reveal the topics of interest of cyber security research for governments. Similarly, government contractors may be supporting agencies in topics such as computer security where no government involvement was found in the institution in the dataset.

## 5.8 Cyber security aspects in the next few years

Studying what institutions classified into the cyber security aspect dimension are doing sheds light on incipient topics in cyber security. For instance, now that more and more services are based on cloud computing platforms, companies are starting to develop products to secure cloud computing, building on data, network and computer security capabilities. Amazon and Armor are two companies in the dataset offering such products.

Similarly, there are companies, such as Gemalto, working on securing data transfer and processing between different types of hardware. In fact, an increasing number of organizations offer services for securing connections and identity management between different devices such as smartphone, tablets, notebooks, industrial automation systems, wearable devices and other internet of things gadgets. In the next years, the integral management of data security between multiple devices will probably become key to secure software and online services.

For the activity sector, jurisdiction and institutional characteristics dimensions,

[5] In early 2016, the FBI wanted Apple to develop software to help them recover information from an iPhone. Apple refused and the FBI took Apple to court

only the new or incremental insights are going to studied and and analyzed in the next sections.

# 6 The many activity sectors in the dataset

This section studies the clusters in the activity sector dimension. This dimension groups clusters that distinguish institutions in the dataset by the main sector in which their activity takes place: Intelligence, Internet Governance, Internet Policy, Financial Sector, Online Service, Software Hardware and Service Provider and Telecommunications. There are 47 institutions in the dataset that are classified in at least one of the activity cluster. Table 3 shows a sample of institutions in the seven different clusters of this dimension and their governance.

## 6.1 Clusters in the Activity sector dimension

There are seven clusters in the activity sector dimension and 52 institutions from the dataset are classified in them. Figure 8 depicts the proportional size of each cluster in this dimension. The largest cluster is the software, hardware and service providers with 18 institutions, followed by Internet policy with 14 and telecommunications with nine. The smallest clusters are the intelligence and financial sectors with three and four institutions respectively.

Most of the clusters in this dimension are dominated by one type of institution with the exception of the telecommunication cluster where there is a mix of institutions. This is mainly because telecommunications is a highly regulated sector with international agreements being the instrument that allowed telecommunication cable connections globally. Therefore, there are for-profit and not-for-profit private actors, government agencies and international organizations in the telecom cluster. In contrast, the software, hardware and services provider and the online services are composed of private sector institutions only and mostly for-profit organizations. The Internet governance and Internet policy clusters are dominated by not-for-profit institutions, the big contributors to the Internet development. The intelligence sector is composed by government institutions only, the security agencies. The few institutions in the financial cluster are of many different types. However, there is not enough data to make conclusions.

There are 11 institutions that are classified in two activity sector clusters and most of them link sectors where the boundaries are blurry. Figure 9 reveals these connections with red links for institutions that are in two clusters. We can see that

| Institution | Cluster | Governance |
|---|---|---|
| GCHQ : Government Communications Head Quarters UK | Intelligence | Government |
| NSA : National Security Agency | Intelligence | Government |
| ICANN : Internet Corporation for Assigned Names and Numbers | Internet Governance | Not-for-profit |
| LACNIC : Latin American and Caribbean Internet Addresses Registry | Internet Governance | Not-for-profit |
| Symantec | Computer Security | For profit |
| OECD : Organization for Economic Co-operation and Development | Internet Policy | Treaty Organization |
| FCC : Federal Communications Commission | Internet Policy | Government |
| FSSCC : Financial Services Sector Coordinating Council | Financial Sector | Government |
| PayPal | Financial Sector | For profit |
| CloudFlare | Online Services | For profit |
| Google | Online services | For profit |
| Microsoft Corporation | Soft., Hardware and Service Providers | For profit |
| Mozilla Foundation | Soft., Hardware and Service Providers | Not-for-profit |
| AT&T | Telecommunications | For profit |
| ETSI : European Telecommunications Standards Institute | Telecommunications | Not-for-profit |

Table 3: Sample of institutions in clusters of the activity sector dimension.

the Internet policy clusters shares many institutions with the Internet governance and telecommunications clusters. Additionally, the online services and software, hardware and services providers clusters have many institutions in common.

There are 73 institutions in the dataset that are not classified in any cluster of the activity sector dimension. These institutions are mainly government agencies, international organizations and not-for profits that are not sector specific but that participate of the cyber security ecosystem. For instance, the National Institute of Standards and Technology in the US, the World Trade Organization and the Anti-Phishing Working Group do not have a specific sector they work for but have working groups focusing on cyber security.

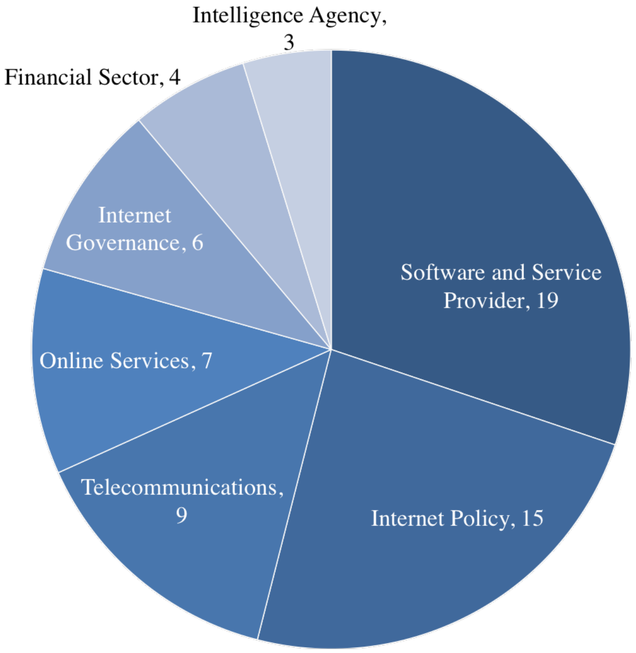

Figure 8: Number of institutions in each cluster of the activity sector dimension.

## 6.2 Cross-cutting other dimensions by activity sectors

There are 27 institutions in the activity sector dimension that are also in the cyber security aspect clusters. In fact, most companies in the software, hardware and service provider cluster are also part of the computer, data or network security clusters from the cyber security aspect dimension. Some institutions from the Internet policy, Internet governance and telecommunication clusters are also part of the network security cluster. The other 24 institution in this dimension do not have a specific focus in cyber security, their approach is as a whole from their activity sector point of view, such as the National Institute of Standards and Technology that covers many different areas.

There are few institutions in the activity sector dimension that are also part of a jurisdiction cluster. The US is the most represented jurisdiction with institutions in the financial sector, intelligence, Internet policy and telecommunication sector. Moreover, in the telecommunication sector there are institutions from the US, European Union, Asia-Pacific and Asia.

Finally, many companies in the activity sectors are also part of the consumer oriented cluster. These companies focus primarily on cyber security to protect users

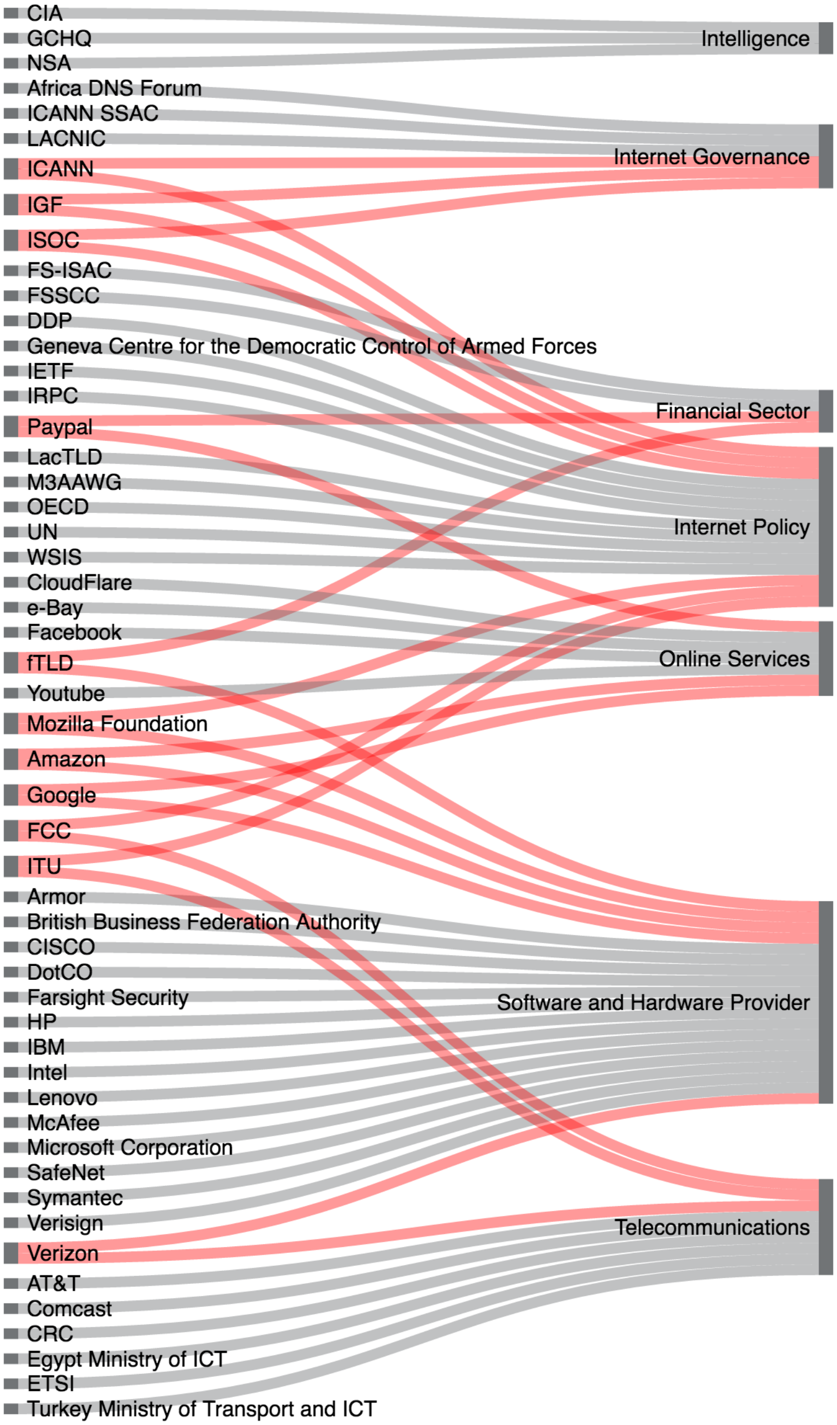

Figure 9: Institutions in activity sector dimension's clusters. Red links indicate institutions in more than one cluster.

from possible harm that would make users not use their products and services. eBay, PayPal and Facebook are a few examples.

### 6.3 Missing institutions and future activity sector clusters

Most institutions in the dataset with a specific activity sector have an activity linked to the development of the Internet ecosystem: telecommunications, hardware and software providers, online services, Internet policy and governance. The only two sectors that are not a core part of the ecosystem are the financial and intelligence sectors. However, these sectors have been leveraging the development of the Internet infrastructure for their own activities for many years now and have influenced the ecosystem.

There are many more activity sectors where organizations are increasingly leveraging the Internet to provide new products and services. These institutions are not (fully) integrated in the ecosystem. More targeted publications and conferences would need to be surveyed to find the institutions in areas such as automated vehicles, education, e-governance, medical devices and connected devices in general. In the next few years, we can expect many of those activity sectors to become more connected to the rest of the institutions as their products get more integrated with the ecosystem.

## 7 Jurisdictions in the dataset

The jurisdiction dimension groups clusters that capture a specific geographical zone linked to institutions. The two main clusters of the jurisdiction dimension are the United States (US)and the European Union (EU). Indeed, the US and the EU are among the first governments to include cyber security in their national strategy and to begin organizing the various agency efforts inside their respective governments. The third cluster of the jurisdiction category, Other Regions, can in fact be divided into at least three smaller clusters: Latin America, Asia-Pacific and Africa. However, even summing up the institutions in these three regions, there are fewer institutions from those areas than the US or EU. These institutions were therefore combined into a single cluster called Other Regions. Table 4 shows a sample of institutions in the different clusters of this dimension and their governance.

| Institution | Cluster | Governance |
|---|---|---|
| DoD : Department of Defense | United States | Government |
| FCC : Federal Communications Commission | United States | Government |
| NCSA : National Cyber Security Alliance | United States | Not-for-profit |
| CENTR : Council of European Top Level Domain Registries | Europe | Not-for-profit |
| DG CONNECT : EU Directorate General for Communications Networks, Content and Technology | Europe | Government |
| ENISA : European Union Network and Information Security Agency | Europe | Not-for-profit |
| Egypt Ministry of Communication and Information Technology | Other Regions | Government |
| KISA: Korean Internet and Security Agency | Other Regions | Government |
| LacTLD : Latin American and Caribbean ccTLDs Association | Other Regions | Not-for-profit |

Table 4: Sample of institutions in clusters of the jurisdiction dimension.

## 7.1 Clusters in the jurisdiction dimension

There are three clusters in the jurisdiction dimension: the US, Europe and other regions. The US and EU clusters have almost double as many institutions as the other region cluster combining Asia-Pacific, Africa and Latin America. Figure 10 shows the proportional size of each cluster with the institution counts.

Although the US and the Europe clusters have almost the same number of institutions, their composition is quite different. For instance, the US cluster is mostly composed of government agencies. There is only one institution that is not part of the government, a not-for-profit institution that collaborates closely with the government. In contrast, in the European cluster, there are treaty organizations at the EU and Europe level, governmental organizations part of the EU governance system, and not-for-profit institutions that not only collaborate with the government, but have been mandated by the EU governance system to develop standards.

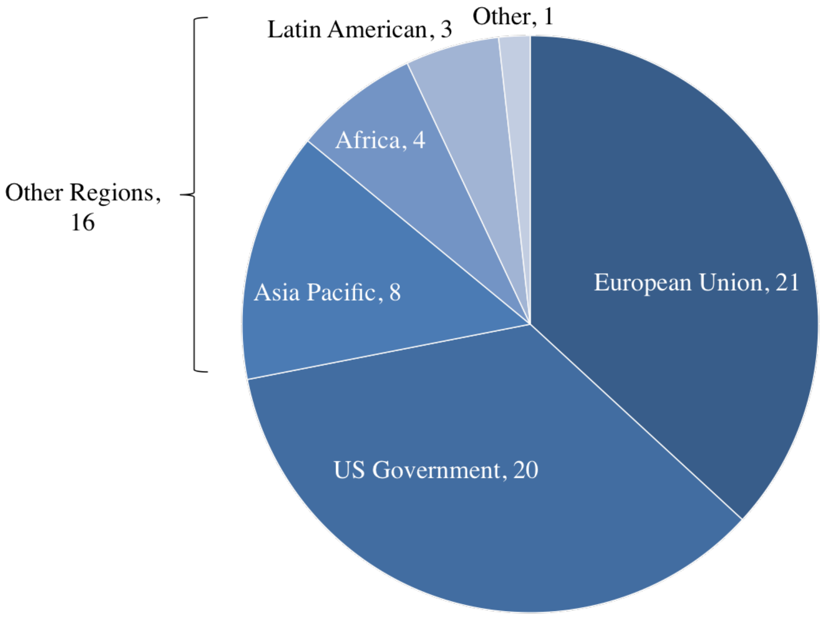

Figure 10: Number of institutions in each cluster of the jurisdiction dimension.The other regions cluster is expanded to show the institutions from the Asia Pacific, Africa and Latin America regions.

## 7.2 Relationship with other dimensions

The US and Europe clusters both have institutions that span across almost all the cyber security aspects. The US has a noticeable concentration of institutions sharing cybercrime effort. Most European institutions are in the cybercrime, security standards and network security clusters. Furthermore, US institutions are more specific in terms of activity sector than European institutions. Indeed, only two European institutions are classified in the activity sector dimension, whereas there are five US institutions in four activity sector clusters.

The institutions from other regions are different from the ones in the US and Europe. To start, most of them are treaty-based organizations that group a few countries together, or not-for-profit institutions linked to Internet registries regions. Additionally, most institutions are in the cybercrime and network security cluster. The Regional Internet Registries and top-level manager association of Asia-Pacific, Africa and Latin America, part of the Internet governance cluster, play relevant roles of training and capacity building in those regions.

### 7.3 Missing institutions and future activity sector clusters

Although in the dataset we included institutions scraped from the IGF 2014 meeting that took place in Istanbul, most institutions in the dataset are *western* institutions. There are a few from India and other parts of the world. However, there might be many more institutions from other parts of the world that should be included in the dataset. Starting from the few institutions found from other regions, the work could be expanded by studying what else is being done in other places and which institutions are relevant. One challenge though is that without knowledge from the Internet ecosystem in the different parts of the world -how the Internet is used, integrated (or not) in every day life and the infrastructure supporting it is run-, it is difficult to evaluate if what institutions are doing there is really shaping Internet security in that region at least.

Nonetheless, institutions from other countries will probably increase their participation in relevant global meetings and conferences covering cyber security and the regions will become better known.

## 8 Other recurrent institution characteristics in the dataset

The last dimension to study is the institutional characteristics dimension. This dimension is different from the other ones and gives information about how and why institutions are working on cyber security. It has five clusters that can be distinguished in two groups: the forum, information sharing and working groups clusters that correspond to modes of operation of institutions, and the consumer oriented and economic focus clusters, which are drivers that got institutions into cyber security. Table 5 shows a sample of institutions in the different clusters of this dimension and their governance.

For many institutions in the cyber security ecosystem, Information sharing of vulnerabilities, security incidents and related statistics is a key mode of operation. Other institutions are Forums that bring members together to discuss and decide on best practices, solutions and policies. And for many institutions, cyber security is a secondary objective and they have a specific Working group, item or unit working in the cyber security areas that are relevant for the main objective of the institution. For example, the World Trade Organization's objective is to set the rules of trade between countries, and it has two working groups that are involved in cyber security as it is relevant for part of the trade rules and agreements between countries: international

| Institution | Cluster | Governance |
|---|---|---|
| US-CERT : United States Computer Emergency Readiness Team | Information Sharing | Government |
| SAFECode : Software Assurance Forum for Excellence in Code | Information Sharing | Not-for-profit |
| APEC : Asia-Pacific Economic Cooperation | Forum | Treaty Organization |
| NANOG : North America Network Operators Group | Forum | Not-for-profit |
| ISO : International Organization for Standardization | Working Group | Not-for-profit |
| World Trade Organization | Working Group | Treaty Organization |
| Facebook | Consumer Oriented | For profit |
| FTC : Federal Trade Commission | Consumer Oriented | Government |
| DG GROWTH : EU Directorate General for Internal Market, Industry, Entrepreneurship and SMEs | Economic Focus | Government |
| OECD : Organization for Economic Co-operation and Development | Economic Focus | Treaty Organization |

Table 5: Sample of institutions in clusters of the institution characteristic dimension.

trade and Internet privacy, and international trade and national security. Similarly, some institutions are Consumer oriented  and for them the consumer is central to their organization. Finally, other institutions have an Economic focus and economic growth and prosperity is central to their main objective. Figure 11 shows the count of institutions in each cluster of this dimension.

The forum institutions are either treaty organizations, where representatives from different governments discuss and agree upon common terms for dealing with cyber security issues, or not-for-profit institutions that provide a space of discussion, debate and agreement between different actors in many topics of cyber security. Information sharing institutions are similar to forum institutions but are more focused on the exchange of information about incidents, statistics and experience than in the discussion and setting of common standards or understanding frameworks (especially for cyber crime). There are not-for-profit, government and treaty based organizations in this cluster. Institutions in the working group cluster are institutions whose core activities are not directly related to cyber security and the organization decided to cover cyber security through the work of a somewhat independent working group. The

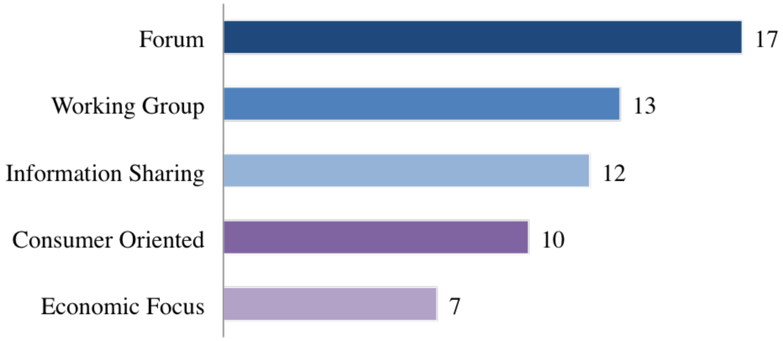

Figure 11: Number of institutions in each cluster of the institution characteristic dimension. Modes of operation in blue and interests in purple.

institutions in this cluster are mainly not-for-profit and international organizations with a high level objective for which it became relevant to work on cyber security. For instance, the World Trade Organization has a working group on international trade and Internet privacy.

Consumer oriented institutions are either government agencies in charge of consumer protection, such as the Federal Trade Commission in the US, or companies whose focus on cyber security comes from protecting the user from potential harm that could happen when using their product or service, such as Facebook. Economic focus institutions are mainly treaty organizations put in place to foster economic growth within a region or group of countries. These institutions became interested in cyber security because of its increasing relevance in economic security.

There are clusters that have many forums or information sharing institutions. In the next years, to prevent competing with similar institutions, these institutions could collaborate and leverage the members of all institutions together.

# 9 Conlcusions

Starting from government and international organization documents, and using automated tools to extract institution names from conference discussions in cyber security, a dataset of 124 institutions was built. The institutions in the dataset are shaping internet security by their ability to influence policy and regulation of cyber security or directly the security of internet users. The dataset is composed of very different institutions in terms of governance, activity, mode of operation, relation to cyber security and scope.

To gain insights about the landscape of institutions in the dataset, a framework of 28 aspects organized in five dimensions is proposed (Figure 1). It separated the different types of characteristics in cyber security aspects, activity sectors, jurisdictions, institutional characteristics, and governance types.

Since the time the initial analysis was done and the dataset built, more institutions have emerged that could be added to the dataset and classified in the clusters of the framework. Additionally, more institutions will emerge in the future that will probably add new aspects to some dimensions of the framework. However, it is unlikely that categories would be erased in the medium term.

The framework of cluster is a useful tool to untangle the rich and diverse underlying structure of institutions shaping cyber security, contributing to understanding the different perspective and incentives of institutions with respect to cyber security. Studying the institutions in the different clusters in each dimension and cross cutting with the other dimensions revealed the trends and roles institutions have in the ecosystem.

## 9.1 The landscape of cyber security institutions

The landscape of institution shaping cyber security is a rich ecosystem with institutions of varied nature. The institutions we included in the dataset focus mainly on nine areas of cyber security: network security, cybercrime, security standards, data security, data protection, computer emergency response, computer security, cyber security research and cyber defense, in descending number of institutions involved in each aspect. There are other aspects of cyber security that appeared in nascent form, such as cloud computing security and multi-platform security, that will probably become relevant in the next years.

Additionally, the institutions found come from mainly seven activity areas: hardware, software and service providers, Internet policy, telecommunications, online services, Internet governance, financial sector and intelligence; from the most to the least common in institutions. The distinction between these activity sectors is sometimes weak and will probably continue to merge as more sectors converge. New topics such as the Internet of Things and automated vehicles will probably make it onto the list very soon.

For-profit and not-for-profit private institutions, government institutions and international treaty organization are all well-represented in the ecosystem. The private sector accounts for over 50% of institutions, with not-for-profit organizations being the largest share.

In terms of geographical scope, the two main areas of institutions shaping cyber security are the US and Europe, although a few institutions come from Asia-Pacific, Africa and Latin America. Probably many more institutions from these other regions are going to be part of the ecosystem in the near future.

Three usual modes of operation in the institutions included in the dataset are identified. Many institutions are forums, where members discuss views and experiences to come up with consensus of best practices. Another large share of institutions are a point of information sharing between members, exchanging incidents reports, statistics, experiences and best practice informations. For many institutions, cyber security is not a core area of expertise and they develop their work in cyber security in a somewhat independent working group of experts. Similarly, in institutions whose primary objective is not directly related to security, we identify two main reasons for getting involved in cyber security. Institutions that are consumer oriented with products that rely significantly on the Internet infrastructure, or that are concerned about possible harm to users, start caring about cyber security to preserve consumer trust and limit their harm. Likewise, organizations concerned by economic development have begun to realize the relevance of Internet infrastructure security in economic security and thus have started initiatives in cyber security.

In each of these dimensions of study, the aspects of cyber security covered, activity sector, governance, geographical scope and other institutional characteristics, groups of institutions can be very different between them, one more geared toward one topic, or one activity sector than another, with more or less private or public institutions, with institutions from one part of the world instead of another. No two clusters of institutions are really similar, and the distribution of institutions in definitely not uniform in any dimension, with usually no institution having an established leadership position in cyber security topics. This systemic study allowed us to better understand the different perspectives, incentives and roles of institutions in the large and rich ecosystem that constitutes the institutional landscape of cyber security.

## 9.2 Future work

Using this work as foundation, there are three main directions for future work: expanding the dataset, using the framework to study a specific topic in cyber security, and studying the emerging topics that are not visible in the framework. The dataset could be expanded by using other sources of information. For instance, papers presented in cyber security conference could be scraped to find sources of funding.

Indeed, in the current dataset very few institutions are invested in cyber security research. However, it is an activity usually outsourced through contracts and grants to research institutions. It would be interesting to map were funds in cyber security research are being allocated.

Furthermore, picking specific topics in cyber security, a more detailed studied of institutions involved could be done to better understand how institutions in different clusters interact with each other. For example, if we would be interested in understanding which institutions would participate in improving home routers' security, we could take a look at institutions in the network security, data protection, hardware providers, telecommunications and consumer oriented clusters as these aspects are directly related to home router security. There are 14 institutions in the dataset that are in two or more of those clusters that could be a starting point to investigate the issue. Taking another approach, we could take all institutions in the cluster whose scope appears to cover home router security and study the common aspect of these institutions. In the dataset, 20 institutions have a scope that covers home router security. As expected, many institutions are in the clusters mentioned above. It is interesting to note that there is one forum institution, the Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG), that appears to do related work in its effort agains botnets, malware, spam, and other online exploitations. It could be a good lead to gain multistakeholder involvement in the issue.

Finally, there are cyber security aspects that are not in the framework because just one or two institutions in the dataset, such as cloud computing and securing identity management across multiple platforms. Probably more institutions are working on those topics. It would be interesting to find out who they are and how they would fit in the current landscape.

# References

[1] N. Choucri, S. Madnick, and J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development*, vol. 20, pp. 96–121, Apr. 2014.

[2] D. K. Mulligan and F. B. Schneider, "Doctrine for Cybersecurity," *Daedalus*, vol. 140, pp. 70–92, Sept. 2011.

[3] A. Sofaer, D. Clark, and W. Diffie, "Cyber Security and International Arrangements," National Academic Press, 2010.

[4] OECD, “Cybersecurity Policy Making at a Turning Point,” OECD Digital Economy Papers, Organisation for Economic Co-operation and Development, Paris, Nov. 2012.

[5] OAS, “Report on Cybersecurity and Critical Infrastructure in the Americas,” tech. rep., Organization of American States, Trend Micro, Apr. 2015.

[6] S. Purser, “Standards for Cyber Security,” *Best Practices in Computer Network Defense: Incident Detection and Response*, vol. 35, no. 2014, pp. 97–106, 2014.

[7] C. Testart, “Understanding the Institutional Landscape of Cyber Security,” June 2016.

[8] “Reform of EU data protection rules - European Commission.”

[9] “European Council approves EU General Data Protection Regulation draft; final approval may come by end of 2015.”

[10] U. S. D. of Defense, “THE DEPARTMENT OF DEFENSE CYBER STRATEGY,” tech. rep., US Department of Defense, Apr. 2015.

[11] D. D. Clark, “Control Point Analysis,” SSRN Scholarly Paper ID 2032124, Social Science Research Network, Rochester, NY, Sept. 2012.

[12] C. for International Governance Innovation and C. House, “Toward a Social Compact for Digital Privacy and Security, Statement by the Global Commission on Internet Governance,” tech. rep., CIGI, Chatham House, 2015.

[13] C. for Democracy & Technology, “Unpacking ”Cybersecurity”: Threats, Responses, and Human Rights Considerations,” June 2013.

[14] WSIS, “TUNIS AGENDA FOR THE INFORMATION SOCIETY,” Nov. 2005.

[15] IGF, “The Global Multistakeholder Forum for Dialogue on Internet Governance Issues,” tech. rep., Internet Governance Forum, 2014.

[16] IGF, “IGF 2014 Finished transcripts,” 2014.

[17] OECD, “An overview of the digital economy,” in *OECD Digital Economy Outlook 2015*, pp. 15–82, OECD Publishing, July 2015.

[18] S. Bird, E. Klein, and E. Loper, *Natural Language Processing with Python - Analyzing Text with the Natural Language Toolkit.* O’Reilly Media Inc., 2009.

[19] S. Osinski and D. Weiss, “A concept-driven algorithm for clustering search results,” *IEEE Intelligent Systems*, vol. 20, pp. 48–54, May 2005.

[20] D. P. Fidler, “Introductory Note to the Final Acts of the World Conference on International Telecommunications,” *International Legal Materials*, vol. 52, no. 3, pp. 843–860, 2013.

[21] OECD, *Digital Security Risk Management for Economic and Social Prosperity.* OECD Publishing, Oct. 2015.

[22] D. Clark, “The Landscape of Cyber-security,” May 2015.

[23] “OPEN DATA CENTER ALLIANCE USAGE: Data Security Framework Rev 1.0,” 2013.

[24] NW3C, “National White Collar Crime Center Annual Report 2014,” tech. rep., 2015.

[25] C. François, J. Ben-Avie, D. Steer, and S. Midghall, “Mozilla Cybersecurity Delphi 1.0: Towards a user-centric policy framework,” tech. rep., July 2015.

[26] Ministy of Science, ICT, and Future Planning and Korea Internet and Security Agency, “Korea Internet White Paper 2015,” tech. rep., 2015.

[27] T. W. House, “Executive Order – Improving Critical Infrastructure Cybersecurity,” Feb. 2013.

[28] E. Commission, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” July 2013.

# A List of Institutions in the Dataset

The final list of institutions included in the dataset studied for this work is in table 6 as well as the clusters each institution is in.

Table 6: List of institutions in the dataset.

| Name | Governance | Other Clusters |
|---|---|---|
| Africa DNS Forum | Not-for-profit | Africa, Forum, Internet Governance |
| African Union | Treaty Organization | Africa, Data Protection, Cybercrime |
| AfTLD: Africa Top Level Domains Organization | Not-for-profit | Africa, Network security |
| AISI : Australian Internet Security Initiative | Government | Network Security, Asia Pacific |
| Amazon | For profit | Data Security, Software and Service Provider, Online Service |
| AP-CERT : Asia Pacific Computer Emergency Response Team | Treaty Organization | Computer Emergency Response Team, Asia Pacific, Information Sharing |
| APEC : Asia-Pacific Economic Cooperation | Treaty Organization | Asia Pacific, Economic Focus, Forum, Working group |
| APNIC: Asia-Pacific Network Information Centre | Not-for-profit | Asia Pacific, Network security |
| APWG : Anti-Phising Working Group | Not-for-profit | Cybercrime, Information sharing |
| Armor : FireHost | For profit | Software and Service Provider, Data Security |
| ASEAN : Association of South Asian Nations | Treaty Organization | Economic Focus, Asia Pacific, Cybercrime, Working group |
| AT&T | For profit | Network Security, Telecommunications |
| British Business Federation Authority | Not-for-profit | Software and Service Provider, Data Security |
| CAIDA : Center for Applied Internet Data Analysis | Not-for-profit | Cyber Security Research |
| CEN : European Committee for Standardization | Government | Security Standards, Europe |
| CENELEC : European Committee for Electrotechnical Standardization | Not-for-profit | Security Standards, Europe |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| CENTR : Council of European Top Level Domain Registries | Not-for-profit | Network Security, Europe |
| CERT/CC : CERT Coordination Center | Not-for-profit | Computer Emergency Response Team, Cyber Security Research |
| CERT/EU : Computer Emergency Response Team European Union | Government | Europe, Computer Emergency Response Team, Information Sharing |
| CIA : Central Intelligence Agency | Government | Intelligence Agency, United States |
| CISCO | For profit | Network Security, Software and Service Provider |
| CloudFlare | For profit | Online Services, Network security |
| Comcast | For profit | Telecommunications, Network security |
| Commonwealth Cybercrime Initiative | Treaty Organization | Cybercrime |
| ConnectSafely | Not-for-profit | Consumer Oriented |
| Council of Europe | Treaty Organization | Europe, Cybercrime |
| CRC : Colombian Communications Regulation Commission | Government | Telecommunications |
| DDP : Digital Defenders Partnership | Not-for-profit | Internet Policy |
| DG CONNECT : EU Directorate General for Communications Networks, Content and Technology | Government | Europe, Network Security |
| DG DIGIT : EU Directorate General for Informatics | Government | Europe |
| DG GROWTH : EU Directorate General for Internal Market, Industry, Entrepreneurship and SMEs | Government | Europe, Security Standards, Economic Focus |
| DG HOME : EU Directorate General Home Affairs | Government | Europe, Cybercrime |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| DG JUST : EU Directorate General for Justice and Consumers | Government | Europe, Data Protection, Consumer Oriented |
| DHS : Department of Homeland Security | Government | Network Security, United States, Cybercrime, Data Security |
| DoD : Department of Defense | Government | Network Security, Cyber Defense, United States |
| DoJ : Department of Justice | Government | United States, Cybercrime |
| DoS : Department of State | Government | United States |
| DotCO : Colombia's Top level Domain | For profit | Software and Service Provider |
| DSCI : Data Security Council of India | Not-for-profit | Data Protection |
| e-Bay | For profit | Online Services, Consumer Oriented |
| EC JRC : European Commission Joint Research Center | Not-for-profit | Cyber Security Research, Europe, Working Group |
| EDA : European Defense Agency | Government | Europe, Cyber Defense, Working Group |
| EDPS : European Data Protection Supervisor | Government | Europe, Data Protection |
| EEAS : European External Action Service | Government | Europe, Cybercrime |
| Egypt Ministry of Communication and Information Technology | Government | Telecommunications, Africa |
| ENISA : European Union Network and Information Security Agency | Government | Network Security, Europe, Data Protection |
| ETSI : European Telecommunications Standards Institute | Not-for-profit | Europe, Security Standards, Telecommunications |
| EUISS : EU Institute for Security Studies | Not-for-profit | Europe, Cyber Security Research |
| European Commission | Treaty Organization | Europe |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| European Parliament | Treaty Organization | Europe |
| EUROPOL : European Police Office | Treaty Organization | Europe, Cybercrime |
| Facebook | For profit | Online Services, Consumer Oriented |
| Farsight Security | For profit | Network Security, Software and Service Provider |
| FBI : Federal Bureau of Investigation | Government | United States, Cybercrime |
| FCC : Federal Communications Commission | Government | United States, Internet Policy, Telecommunications |
| FIRST : Forum for Incident Response and Security Teams | Not-for-profit | Computer Emergency Response Team, Forum |
| FS-ISAC : Financial Sector Information Sharing and Analysis Center | Not-for-profit | Financial Sector, Computer Emergency Response Team, Information Sharing |
| FSSCC : Financial Services Sector Coordinating Council | Government | Financial Sector, United States |
| FTC : Federal Trade Commission | Government | United States, Data Protection, Consumer Oriented |
| fTLD | For profit | Software and Service Provider, Financial Sector |
| G7 : Group of Seven (formerly Group of Eight) | Treaty Organization | Forum, Cybercrime, Working Group |
| GCHQ : Government Communications Head Quarters UK | Government | Intelligence Agency, Data Security, Europe |
| Geneva Centre for the Democratic Control of Armed Forces | Not-for-profit | Internet Policy, Working group |
| GICSR : Global Institute for Cybersecurity + Research | Not-for-profit | Cyber Security Research, Information sharing |
| Google | For profit | Online Services, Software and Service Provider, Consumer Oriented |
| HP | For profit | Software and Service Provider, Computer Security |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| IBM : IBM Corporation | For profit | Software and Service Provider, Data Security, Network security |
| IC3 : Internet Crime Complaint Center | Government | United States, Cybercrime |
| ICANN : Internet Corporation for Assigned Names and Numbers | Not-for-profit | Internet Governance, Network security, Internet Policy |
| ICANN SSAC : Security and Stability Advisory Committee of ICANN | Not-for-profit | Internet Governance, Network security |
| ICS CERT : US Industrial Control Systems Cyber Emergency Response Team | Government | United States, Computer Emergency Response Team, Information Sharing |
| IEC : International Electrotechnical Commission | Not-for-profit | Security Standards |
| IEEE : Institute of Electrical and Electronics Engineers | Not-for-profit | Forum, Security Standards |
| IETF : Internet Engineering Task Force | Not-for-profit | Security Standards, Network Security, Internet Policy |
| IGF : Internet Governance Forum | Treaty Organization | Internet Governance, Forum, Internet Policy |
| IMPACT : International Multilateral Partnership Against Cyber Threats | Treaty Organization | Forum, Information sharing, Computer Emergency Response Team |
| Intel | For profit | Computer Security, Software and Service Provider |
| Intel Security Group - McAfee | For profit | Software and Service Provider, Network Security, Computer Security, Data Security |
| INTERPOL : International Criminal Police Organization | Treaty Organization | Cybercrime |
| IRPC : Internet Rights and Principles Coalition | Treaty Organization | Internet Policy |
| ISO : International Organization for Standardization | Not-for-profit | Security Standards, Working group |
| ISOC : Internet Society | Not-for-profit | Internet Governance, Internet Policy |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| ITU : International Telecommunication Union | Treaty Organization | Internet Policy, Telecommunications |
| Korean Internet and Security Agency | Government | Data Security, Data Protection |
| LACNIC : Latin American and Caribbean Internet Addresses Registry | Not-for-profit | Latin American, Network Security, Internet Governance |
| LacTLD : Latin Americanand Caribbean ccTLDs Association | Not-for-profit | Network Security, Internet Policy, Cybercrime, Latin American |
| LAP : London Action Plan | Not-for-profit | Forum, Data Protection |
| Lenovo | For profit | Computer Security, Software and Service Provider |
| M3AAWG : Messaging, Malware, Mobile Anti-Abuse Working Group | Not-for-profit | Forum, Internet Policy, Network security |
| Microsoft Corporation | For profit | Software and Service Provider, Consumer Oriented, Computer Security |
| Ministry of Administration and Digitization of Poland | Government | Data Protection |
| Mozilla Foundation | Not-for-profit | Software and Service Provider, Internet Policy, Working Group |
| NANOG : North America Network Operators Group | Not-for-profit | Network Security, Forum |
| NATO : North Atlantic Treaty Organization | Treaty Organization | Cyber Defense |
| NCSA : National Cyber Security Alliance | Not-for-profit | Consumer Oriented, United States |
| NIST : National Institute of Standards and Technology | Government | Economic Focus, Security Standards, United States |
| NSA : National Security agency | Government | Intelligence Agency, United States |
| NW3C : National White Collar Crime Center | Not-for-profit | Cybercrime, United States |
| OAS : Organization of American States | Treaty Organization | Forum, Working group, Cybercrime |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| OASIS : Organization for the Advancement of Structured Information Standards | Not-for-profit | Security Standards, Forum |
| ODCA : The Open Data Center Alliance | Not-for-profit | Security Standards, Forum, Data Security |
| OECD : Organization for Economic Co-operation and Development | Treaty Organization | Working group, Internet Governance, Economic Focus |
| Paypal | For profit | Online Services, Financial Sector, Consumer Oriented |
| SAFECode : Software Assurance Forum for Excellence in Code | Not-for-profit | Forum, Information sharing |
| SafeNet : Gemalto | For profit | Data Security, Data Protection, Software and Service Provider |
| SCO : Shanghai Cooperation Organization | Treaty Organization | Cybercrime, Economic Focus, Asia Pacific |
| Secret Service | Government | United States, Cybercrime |
| Spamhaus | Not-for-profit | Network Security, Information sharing |
| Symantec | For profit | Software and Service Provider, Network Security, Computer Security, Data Security |
| TF-CSIRT : Task Force CSIRT | Not-for-profit | Forum, Computer Emergency Response Team, Information Sharing |
| The Open Group | Not-for-profit | Forum, Security Standards |
| Turkey Ministry of Transport, maritime affairs and communications | Government | Telecommunications, Asia Pacific |
| UAE Cert | Government | Computer Emergency Response Team, Information sharing |
| UN : United Nations | Treaty Organization | Working Group, Internet Policy |
| US Congress | Government | United States |
| US Cyber Command | Government | Cyber Defense, United States |
| US-CERT : United States Computer Emergency Readiness Team | Government | Computer Emergency Response Team, United States, Information Sharing |

Table 6: (continued)

| Name | Governance | Other Clusters |
|---|---|---|
| Verisign | For profit | Network Security, Software and Service Provider |
| Verizon : Verizon Communications | For profit | Network Security, Telecommunications, Software and Service Provider |
| W3C : World Wide Web Consortium | Not-for-profit | Security Standards, Working group |
| White House: US Executive Office of the President | Government | United States |
| World Trade Organization | Treaty Organization | Data Protection, Working Group |
| WSIS : World Summit on the Information Society | Treaty Organization | Internet Policy, Forum |
| Youtube | For profit | Online Services, Consumer Oriented |