GLOBE GLOBAL GOVERNANCE
AND THE EUROPEAN UNION
Future Trends and Scenarios

REPORT

Case study of cyber governance

Project:	GLOBE – The European Union and the Future of Global Governance
GA:	822654
Call:	H2020-SC6-GOVERNANCE-2018
Funding Scheme:	Collaboration Project

Funded by the Horizon 2020 Framework
Programme of the European Union.
Grant agreement number 822654

DISCLAIMER

This project has received funding from the European Union's Horizon 2020 Research & Innovation programme under Grant Agreement no. 822654. The information in this deliverable reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

Due date:	2020-11-30
Submission date:	2020-11-30
Lead beneficiary:	Fundación ESADE
Authors:	Athanasios Kouliopoulos, Marie Vandendriessche, Angel Saz-Carranza

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS

AU	African Union
APWG	Anti-Phishing Working Group
ASEAN	Association of Southeast Asian Nations
BRICS	Brazil, Russia, India, China, and South Africa
CSDP	Common Security and Defence Policy
CERTs	Computer Emergency Response Teams
CIA	Confidentiality, Integrity, Availability
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CoW	Correlates of War
CIIP	Critical Information Infrastructure Protection
ECSO	European Cyber Security Organization
EC3	European Cybercrime Center
EU	European Union
ENISA	European Union Agency for Cybersecurity
FIGO	Formal Intergovernmental Organization
IGO	Intergovernmental Organization
ITU	International Telecommunication Union
IANA	Internet Assigned Numbers
ICANN	Internet Corporation for Assigned Names and Numbers
IoT	Internet of Things
ISOC	Internet Society
NASA	National Aeronautics and Space Administration
NTIA	National Telecommunications and Information Administration
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
OAS	Organization of American States
PPP	Public Private Partnership
RIRs	Regional Internet Registries
CSIRTs	Security Incidence Response Teams
SCO	Shanghai Cooperation Organization
UN	United Nations
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society

1. Introduction

Over the last decade, cyberattacks have increased in frequency, scale and sophistication, disrupting operations, breaching privacy, and violating intellectual property across the world. According to the most recent annual cybercrime report of Cybersecurity Ventures, recent incidents like the 2018 Marriott data breaches and the 2017 WannaCry and NotPetya attacks have become generally more complex and costlier than previous attacks of the same kind. So much so, that cybercrime is expected to cost the world $6 trillion annually by 2021, which will make it “more profitable than the global trade of all major illegal drugs combined” (Morgan, 2019, p. 2).

Illegal activities of cybercriminals are not the only source of insecurity in cyberspace, nor do cyberattacks only affect the economic profitability of companies. Activities like state-to-state cyberespionage – as of today still unregulated by international public law – may also compromise cybersecurity. Cyberespionage may directly affect a state’s national security. China’s alleged 2015 intrusion at the United States Office of Personnel Management provides a clear example. The unauthorized access to confidential data on millions of former and active US government employees – including information on security clearances for some of the most secretive jobs – is a counterintelligence goldmine for intruders as they can identify covert agents and exploit personal data to recruit informants (Buchanan, 2016, p. 159; Finnemore & Hollis, 2016, p. 431).

While cyberthreats are proliferating at an astonishing rate, actors who respond to them are trying to keep up by creating global and regional governance institutions to mitigate risks and reinforce cybersecurity. For example, the European Union has created the EU Agency for Cybersecurity (ENISA), and actors from both the public and private sector contribute to the World Wide Web Consortium’s working groups for web security standards.

The objective of this working paper is to identify and study the international institutions that govern cybersecurity, focusing particularly on their membership structures and the scope of their activities. We specifically look at international institutions involving a range of different configurations and actors – both public and private – since we are interested in understanding how collective action is sought at a global level in this sensitive and crucial issue area. In this paper, we will characterize the “loosely coupled” set of institutions working on these issues as a regime complex (Keohane & Victor, 2011, p. 7). The institutions that comprise the regime complex, whether public, private or hybrid in membership (Green & Auld, 2017), all aim to govern a specific issue while displaying overlaps and lacking a clear hierarchy.

In the context of the GLOBE project, this mapping exercise will contribute novel data that will allow us to systematically study and compare international institutions governing cybersecurity. In view of the importance of cybersecurity in practically all sectors of human activity, there are surprisingly few efforts to map the governance ecosystem created around this issue area. To the best of our knowledge, there have been three such efforts so far. Portnoy and Goodman (2009) produced a very comprehensive and detailed study about global initiatives to secure cyberspace, yet this area is currently developing rapidly, thus update is warranted. Joseph Nye’s (2014) much-cited paper “Global initiatives to secure cyberspace: An emerging landscape” complements the previous work by using regime complex theory to expand the scope of his study on cybersecurity. Finally, Badiei and Kuerbis (2017) identify the networks, markets and hierarchies that interact in order to produce and govern cybersecurity. Building on these three efforts, this paper creates a new, comprehensive and updated dataset, covering both intergovernmental and transnational institutions, and going beyond the previous maps of institutions by focusing on the institutions' membership, scope, design and governance functions.

The novel dataset presented in this paper contains 85 institutions. An overwhelming majority of them began their work on cybersecurity very recently, within the last two decades. Three main findings stand out from our research. First, there appears to be a tendency to govern issues of cybersecurity from existing global governance institutions rather than to create new ones to exercise these functions. Second, the multistakeholder model of internet governance is only partially replicated in cybersecurity governance, where single membership-type institutions are still prevalent. Third, although the Internet itself – and its original governance – were founded in the private sphere, governmental actors remain highly present in the regime complex.

The paper commences, in section 2, by discussing how the need for cybersecurity governance emerged and then evolved. After this contextualization, we establish the conceptual framework for the paper, specifying and explaining, in turn, the definition of cybersecurity and global cybersecurity governance applied in this study. In section 3, we present a novel dataset on the 85 international institutions that form the cybersecurity regime complex, discussing the data collection process for the population and the variables included in turn. Section 4 presents our findings, first on the overall regime complex for global cybersecurity governance and then on two specific issues: the scope and the membership structure of the cybersecurity initiatives. Section 5 concludes.

2. Cybersecurity and its governance: Emergence and conceptualization

Before examining the global governance of cybersecurity in depth, it is useful to understand how the need for this governance emerged and evolved. The first part of this section therefore provides a brief overview of some of the reasons why security issues have emerged through the spread of the internet, the initial efforts to provide global governance of the internet, and the recent rise of cybersecurity concerns on the global governance agenda. In the second part of this section, we establish the conceptual framework for this paper: we specify and explain, in turn, the definition of cybersecurity and global cybersecurity governance applied in this study.

2.1 The emergence of the governance object and its initial institutionalization

The design of the internet and why it matters

Cybersecurity emerged as a sub-field embedded in computer networks and, above all, the Internet. Hence, in order to explain the nature of cybersecurity challenges and the corresponding efforts to govern those challenges, we start by looking at the design of the Internet and the initial stages of Internet governance.

The Internet as we know it today is both the result of conscious choices made by policy makers (regulatory interventions and government funding) and an interplay of market forces and network externalities that are based on assumptions about human behaviour (Zittrain, 2008, pp. 19–21). We turn first to this latter element.

The Internet was based on a generative model,[1] which prioritized flexibility and fostered innovation, but it was not built with security in mind. Its design was simple, resting upon a set of principles that go beyond engineering, such as the “procrastination principle”, which relies on the assumption that future problems confronting networks can be solved later or by others, and the “trust-your-neighbour approach”, which assumed that people using a network and configuring its endpoints would be more or less competent and benevolent enough so as not to intentionally or negligently disrupt the network (Zittrain, 2008, pp. 30–32).

Indeed, this care-free ethos of the Internet’s early-day pioneers made perfect sense at the beginning. The academics who created the first network only envisioned a simple network that could send data between two points; it was up to the people who were connected to figure out how they wanted to use this network (Singer & Friedman, 2014, p. 18). Considering that from 1969 to 1991 the Internet was only used by educational institutions and non-commercial

[1] Generative systems are those that have been “designed to accept any contribution that followed a basic set of rules” – i.e. the functional requirements of an operating system or the protocols of the internet (van Eeten, 2017, p. 435). To put it simply, the generative model is characterized by its openness to third-party contributions. Built as a generative network, the Internet has welcomed third-party software developers who could write new code that could be tried and shared at very little effort and cost (Zittrain, 2008, p. 16).

entities for the purpose of sharing resources and communicating, there was hardly any reason to mistrust the network's participants and anticipate any reckless behaviour.

As such, the first major cyberattacks, in late 1980s and early 1990s, were basically dismissed by Internet pioneers as outliers in an otherwise well-functioning network of trusted participants. Cyberattacks became more common and complicated after the commercialization of the Internet in the early 1990s, but they were still predominantly the domain of tech-savvy teenagers who were trying to make a point from their basements. However, at the turn of the 21st century, the complacent attitude of the previous decades towards cyberthreats gave way to caution and increasing concern.

Internet governance on the global governance agenda

During the 1990s, there was a widespread sense that the network of networks was radically new and unique, developed thanks to the cooperative efforts and technical expertise of non-state actors. As such, traditional regulatory approaches of public command-and-control rule-making were seen as unsuitable for the regulation of cyberspace (Hofmann et al., 2017, p. 1408). Rather, Internet governance was expected to adhere to the original formula of private, decentralized, inclusive and bottom-up policy-making as proposed by the technical community and the private sector (Internet Corporation for Assigned Names and Numbers, 1999), which played a central role in the early development of the Internet.

Eventually however, the expectations that this type of governance would be effective were not met, and states, working through international organizations, assumed an important role in Internet governance. The first step in this phase was the World Summit on the Information Society (WSIS): following a proposal by the International Telecommunication Union (ITU), the UN General Assembly adopted a resolution to hold a World Summit on the Information Society at the highest possible level in two phases, the first in Geneva in 2003 and the second in Tunis in 2005 (A/RES/56/183).

The first phase of the WSIS, however, failed to deliver an agreement on the future of Internet governance due to the diverging state views about the central organization in this field. The US and the European Union,[2] supported by private industry, argued that the Internet Corporation for Assigned Names and Numbers (ICANN), a private, non-profit corporation formed in 1998 to administer the Internet's names and numbers (e.g. website names like cnn.com and IP addresses),[3] should continue to be the focal point in Internet governance

[2] For more information on the European Union's approach to cybersecurity governance, see Annex 1.

[3] ICANN is a private, non-profit corporation formed in 1998 under contract with the United States government to administer the Internet's critical resources (i.e., names and numbers). ICANN and its Internet Assigned Numbers Authority (IANA) function carry out a number of distinct functions including: allocation of blocks of Internet numbers to regional Internet registries (RIRs) for further distribution; oversight of the Internet's root server system operations; the establishment of policies for introducing new top-level domains to the root system; oversight of domain name assignment, albeit delegated to Internet registrars; assignment of unique protocol parameters; and management of the root zone file (Raymond & DeNardis, 2015, p. 594). From 1998 to 2014, ICANN acted more as a US government contractor rather than an independent, multistakeholder governance institution. Over time, "this special status became increasingly controversial and many stakeholders felt that it was incongruous to allow one national government to have exclusive authority over aspects of Internet governance that are critical to all states and all peoples". In 2014, the U.S. Commerce Department announced its intention to end its oversight role and transfer

through its narrowly defined technical mandate. A group of states led by China and other members of the BRICS like Brazil, South Africa and India, however, pushed for a broader understanding of Internet governance and wished to "move the whole internet management system under the umbrella of an intergovernmental organization of the United Nations, notably the International Telecommunication Union" (Kleinwächter, 2004, pp. 233–234).

After the failure of the first phase, the UN Secretary-General established a Working Group on Internet Governance (WGIG)[4] to advance work going into the second phase of the WSIS. The WGIG's report, published in 2005, provided real progress. Until then, Internet governance was largely understood as covering only the management of internet identifiers; it was essentially "a policy space dominated by the internet technical community, the trademark lobby and a few specialists focused on domain names and IP addresses" (Mueller, 2017, p. 415). The WGIG broke new ground in two ways. For one, its definition of Internet governance expanded the scope of actors that can shape the evolution of the Internet: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (WGIG, 2005, p. 4). For another, it recognized that the new understanding of Internet governance that was emerging at the time went well beyond the management of critical Internet resources and included policy domains such as content regulation, shaping the conduct on large-scale intermediary platforms, net neutrality, trade in information services, and – most importantly – cybersecurity, privacy and cybercrime (Mueller, 2017, p. 416).

Cybersecurity rises on the agenda

Following the WGIG's logic, there are scholars who view cybersecurity as a policy domain of Internet governance. For example, Mark Raymond and Laura DeNardis have developed an Internet governance taxonomy in which they regard cybersecurity as merely one of six functional areas within Internet governance (Raymond & DeNardis, 2015, pp. 590–592). However, "security is never only about technology. It is political" (DeNardis, 2020, p. 96). As a result, in the fifteen years since WSIS, two competing frames have emerged and are used in different contexts in order to invoke divergent communities of interests, with different values and priorities, even though they refer to the same underlying issues and technologies.[5]

control of the IANA functions to the global multistakeholder community (Mueller & Kuerbis, 2014, p. 1). This commitment was fulfilled in October 2016, when the contract between ICANN and the United States Department of Commerce National Telecommunications and Information Administration (NTIA) to perform the IANA functions officially expired. At that point, the IANA functions were transferred to Public Technical Identifiers (PTI), an ICANN affiliate, formed as a non-profit public benefit corporation.

[4] WGIG was set up by the Secretary-General of the United Nations in accordance with the mandate given to him during the first phase of the World Summit on the Information Society (WSIS), held in Geneva, in 2003. The WGIG comprised 40 members from governments, private sector and civil society, who all participated on an equal footing and in their personal capacity (WGIG, 2005, p. 3).

[5] To provide an example, in 2007, Russian patriotic hackers launched large-scale denial of service attacks against Estonia's government websites and online banking services. Seen through the lens of Internet governance, this was a breach of availability in need of a technical solution that could reinforce the resilience of systems against such attacks. By framing the same underlying problem as a cybersecurity issue, it could be interpreted as an act of aggression against the sovereignty of a state, activating a whole different community (military and diplomats) with totally different values and priorities (deterrence through diplomatic channels).

Funded by the Horizon 2020 Framework
Programme of the European Union.
Grant agreement number 822654

In the context of contemporary cybersecurity policy, “cyber often reduces to cyber war, cyber conflict, and cybersecurity and is used by military and government communities, as well as security researchers. The term “Internet” in this policy context refers more to global technical infrastructure, global multistakeholder governance, and issues of free speech, access, openness, and development” (DeNardis, 2020, p. 191). Other authors go a step further and posit that cybersecurity has gained so much attention that it has eclipsed most other Internet-related policy domains. For example, Milton Mueller argues that cybersecurity has become such a dominant entry point for Internet policy discussions that it has taken “a life of its own as a governance arena” (Mueller, 2017, p. 416).

Concern over cybersecurity started gaining further momentum after the politically motivated cyberattacks against Estonia in 2007. It was the first time that state-sponsored or, at least, state-tolerated hackers launched large-scale denial of service attacks against the institutions and online services of a foreign government (Georgieva, 2020, p. 38). The realization that cyberspace could be weaponized and that the increasing digitalization of government and banking services had been rendering states vulnerable to crippling cyberattacks became a major source of concern among states.

Importantly, cyber offensive capabilities have three commonly cited characteristics that act as risk multipliers. First, compared to all other physical spaces, there are low barriers and entry costs for acquiring disruptive offensive capabilities in cyberspace (Dunn Cavelty & Wenger, 2020, p. 15). While teenagers today are less likely to penetrate NASA’s computers than they were in the late 1980s, governments are not impervious to significant attacks by small groups of hackers or hacktivists. In other words, the resource asymmetries between states and non-state actors are less pronounced and relevant in cyberspace. Second, owing to the design choices made during the development of the Internet, “there is a general assumption that cyberattack has the advantage against cyber defense” (Singer & Friedman, 2014, p. 154). While the amount of “ground” the defender needs to protect grows exponentially, “the attacker only has to get in through one node at just one time to potentially compromise all the defensive efforts” (*ibid*). Third, the infamous attribution problem often makes it extremely challenging to assign responsibility and hold the authors of an attack accountable. States suspected of ordering or supporting cyberattacks often shield themselves behind plausible deniability and cannot be held accountable (Buchanan, 2016, pp. 143–147).

All things considered, state attitudes towards cybersecurity radically changed after 2007. On a discursive level, cyber intrusions and breaches of information started to evolve from technical risk management issues in critical information infrastructure protection into national security issues with a military component. In other words, cybersecurity has moved upwards in the political agenda and expanded sideways as a problem area to a multitude of additional policy domains (Dunn Cavelty & Wenger, 2020, p. 7).

In this working paper, we place the spotlight on this sensitive yet crucial issue on the global agenda, by studying how collective action on cybersecurity is sought at the global level. In the following, we conceptualize cybersecurity and global cybersecurity governance, detailing the definitions applied in this study.

2.2 The concept of cybersecurity

Unlike international security, which is a notoriously slippery and contested concept, cybersecurity is far less ambiguous. A review of the relevant literature shows that there is unanimity that cybersecurity **at its core** refers to the protection of digital information and data (Christou, 2017; DeNardis, 2014; Dunn Cavelty, 2008; Finnemore & Hollis, 2016; Singer & Friedman, 2014). Any definitional controversies focus on how far the boundaries of cybersecurity should be set, rather than on its essence. For example, some authors posit that cybersecurity refers only to the protection of information and communication technologies themselves (Finnemore & Hollis, 2016, p. 431), while others make a case for a definition that goes well beyond the protection of cyberspace and also covers “those that function in cyberspace and any of their assets that can be reached via cyberspace” (Solms & Niekerk, 2013, p. 101).

For the purposes of this paper, we define cybersecurity as a **set of technologies, processes and practices designed to protect networks, computers, programs and data from unauthorized access and breaches of confidentiality, integrity, and availability.**[6]

This wording follows closely a definition developed by leading cybersecurity scholar Myriam Dunn Cavelty (Dunn Cavelty, 2014) and integrates the famous CIA triangle for information security (Singer & Friedman, 2014, pp. 35–36). The reference to **unauthorized access** implies that a cyber problem becomes a cybersecurity issue only if an adversary knowingly engages in illegal activities in order to obtain private information, undermine a system, or prevent its legitimate use. Therefore, it excludes unintentional system breakdowns that may be owed to random human mistakes or software glitches.

The second element of the definition refers to the protection of **confidentiality, integrity and availability** and indicates that our understanding of cybersecurity remains beneath the layer of content. To put it simply, focus will be put only on cybersecurity techniques, processes and practices that authenticate users, protect the integrity of content and respond to denial of service attacks, worms and other threats against the availability of systems. These institutions are vital for protecting and securing content but are **agnostic to the meaning and usage of this content** (DeNardis, 2014, p. 21). So, issues like hate speech, subversive online speech, distribution of child pornography or cyberbullying remain beyond our scope.

At first glance, our definition covers a diverse set of technical cyber issues, including but not limited to: basic computer viruses, spam, phishing, cryptography breaking, network spoofing, IoT hacking, data leakage, and malware-infested computers organized into remote-controlled botnets that can be used to execute large-scale denial of service attacks. Apart from the purely technical challenges, it also covers threats that result from the alleged intersection of Internet security with the military and political security of the state, including cybercrime, cyberespionage, cyberterrorism and cyberconflict (Mueller, 2010, pp. 159–160).

[6] These three aspects are commonly referred to as the CIA triad or CIA triangle.

Funded by the Horizon 2020 Framework Programme of the European Union.
Grant agreement number 822654

2.3 The concept of global cybersecurity governance

As cybersecurity threats rise on the agenda, so has the global governance of those threats. In this paper we build on Keohane and Nye's (2000) definition of governance,[7] thus **we define global governance of cybersecurity as the institutions that guide and restrain collective global activities related to cybersecurity.**

We do not study the entire array of international institutions governing cybersecurity. Instead, we are interested in institutions that are membership-based (involving more than one actor) Not all global governance institutions are collective in nature, although all of these institutions, by definition, must guide collective activities globally to some extent. For example, ICANN is a foundation and not a membership-based organization, thus it is not included in our database. We are interested in membership-based institutions since these are the most common type of global institutions (the Correlates of War dataset, for example, contained 335 intergovernmental organizations in 2014 (Pevehouse et al., 2020), and the UN Treaty Series has recorded over 50,000 international agreements (https://treaty.un.org)) and, given their collective nature, they are notably difficult to create and to operate (Olson, 1965).

Our unit of analysis is, therefore, international membership-based institutions that guide collective global action to provide cybersecurity. Building from a *governance* perspective, we look beyond the purely state-based initiatives to other categories of actors, including the private sector and non-profit organizations. We include, therefore, both intergovernmental and transnational institutions in our analysis. Due to our focus on *global* governance, national institutions are excluded through the criteria of the members being of at least two different states. Similarly, the institutions under study must have at least three members. This excludes bilateral initiatives, which fall outside the scope of what we consider to be *global* governance.[8] The definition employed here does not, in contrast, limit global governance to transcontinental institutions: regional institutions are also considered, as long as they involve at least three actors from minimum two different countries.

The following section describes the methods used to identify the population of organizations engaged in the global cybersecurity governance and the data collection and coding of the variables collected for each organization in the novel dataset presented in this paper.

[7] Keohane and Nye 2000: "By governance, we mean the processes and institutions, both formal and informal, that guide and restrain the collective activities of a group" (Keohane & Nye, 2000, p. 12)

[8] Whereas Intergovernmental Organizations are typically defined as having members from at least three states (Pevehouse at al., 2020), we include both transnational and intergovernmental institutions in our analysis, and therefore apply a different criterion: at least three members from at least two states. By requiring at least three members, we avoid including bilateral initiatives between two states; by requiring at least two states, we avoid capturing purely national initiatives.

3. Data collection

3.1 Population

The objective of this paper is to provide empirical insights on how the global governance institutions that aim to provide cybersecurity are created and function, with a special focus on their membership structures and the scope of their activities. In order to do so, we constructed a novel dataset, consisting of 85 such institutions,[9] based on pre-existing mapping efforts and compilations of governance initiatives, including academic articles, working papers, books and online sources. See Annex 3 for a detailed list of these sources and their characteristics.

From the 258 governance institutions contained in these sources, 118 met the definition of cybersecurity governance presented above (see section 2.3). Further data cleaning, described below, led to a final list of 85 cybersecurity governance institutions.

- In some cases, the five original sources consulted contained both institutions and their *outputs* (such as legal instruments, centres, and working groups). In these instances, we excluded the *outputs* and instead included only the institutions themselves,[10] in order to avoid duplications. Thus, we gave pre-eminence to the organization when both organization and an output produced by it coexisted.[11]

- In 17 cases, the five original sources contained both an intergovernmental organization and its organs, such as subsidiary bodies, working groups, forums, commissions, committees, and offices. For example, the list contained the European Union, but also the European Parliament, the European Commission, and the Council of the European Union. In cases like this, the organs and their subsidiary bodies were dropped, and we only maintained the parent organization, in order to avoid double or triple-counting the same institution.

- By contrast, specialized agencies and accredited centres of excellence are included (e.g. the Cooperative Cyber Defence Centre of Excellence belongs to a network of NATO-accredited Centres of Excellence, but it is not an operational unit belonging to the NATO Command Structure) as separate institutions. While these institutions may owe their original existence, their personnel, and perhaps even their budget to the actions of a parent organization, they usually enjoy significant autonomy as regards the planning and implementation of their activities and have their own governance structures.

For each of the 85 final governance institutions, we have collected general information on the unit (e.g. year of creation, scope, etc.) as well as specific data on their institutional design,

[9] See Annex 2 for the full list of institutions included in the dataset.
[10] The same applies for some initiatives and platforms (e.g. ISOC IoT Security Policy Platform)
[11] In three cases, the five original sources included an output (a legal instrument, in these cases) but not the institution that had created it. For these cases (East African Community, Economic Community of Central African States, Southern African Development Community), we manually replaced the instrument with the organization that generated it.

membership structures and governance functions. Below we provide brief descriptions of the variables contained in the dataset and the elements they include.

3.2 General information per institution

a. **Full name**: We have included the *current* names of all institutions as they appear in their respective websites.[12]

b. **Acronym:** We use the official acronyms as they appear in the institutions' websites.

c. **Year of creation:**

- For formal intergovernmental organizations (FIGOs), information comes from the Correlates of War IGO Codebook.
- For FIGOs that are not included in the CoW database and for all other institutions, information about their year of creation has been retrieved by their respective websites.
- In the rare cases that the year of creation did not appear in the institution's website, we consulted the source from which we drew them.
- When all previous steps failed, we turned to last-resort alternative sources like the institution's official LinkedIn profile.

d. **Year of involvement in cybersecurity governance:**

- For the vast majority of the 63 institutions that are active in multiple issue areas of global governance (see also 'scope, below), their year of creation predates the year that they actually started to work on cybersecurity, often by many decades. To mitigate this issue, we collected data about the year they became involved in cybersecurity, based on their earliest outputs in that governance area.[13]
- The sources used to gather this data include: official documents on cybersecurity produced by the institutions, the institution's webpages, and repositories and other studies on the cybersecurity (this data collection process is further described in annex 3).

e. **Scope:** We have coded institutions according to the nature of their mandates by using two mutually exclusive binary variables: multipurpose and cyber only. For institutions that focus exclusively on the promotion of cybersecurity as we have defined it and do not engage in any other policy areas we have assigned the code 1 under "cyber_only" and 0 for "multipurpose". Conversely, all other institutions that are involved in policy areas other than cybersecurity were assigned the code 1 under "multipurpose" and 0 for "cyber_only".

f. **Headquarters:** The location of an institution's headquarters was retrieved from its website. In almost all cases information was found in the "about" section that contains general information about the institution.

[12] While most institutions still retain the name by which they appear in our five sources, there have been some name changes over the years. In those cases, we have signalled the change and taken note of the original name.
[13] For more information about the types of outputs that were taken into consideration, see Annex 3

3.3 Institutional design

a. **Secretariat**: Binary variable that contains information about whether an institution has its own secretariat (coded as 1) or not (coded as 0). Information on this variable comes from their respective websites.

b. **Treaty-based institutions**: Treaties are understood in the sense of international public law as formal and binding written agreements among actors, namely sovereign states and international organizations, that need to be signed and ratified by prospective members. Such treaties are often constitutive of the formal intergovernmental organizations in our sample.

c. **Contract-based institutions**: This category encompasses governance institutions that are constituted by and draw their authority from a contract rather than a formal international treaty. For example, many famous non-profit cybersecurity-related industry associations like the Anti-Phishing Working Group or Anti-Malware Testing Standards Organization are based on contracts called "articles of association" (or "certificate of incorporation" or "charter document"). Unlike treaties that are governed by international public law, contracts tend to be governed by national law or international private law.

   Regulations and decisions adopted by organs of FIGOs in order to create new agencies are also considered as contracts in this paper. Therefore, the European Union Agency for Network and Information Security (ENISA) created by EU Regulation No 526/2013 of the European Parliament and of the Council has been coded as a contract-based institution.

d. **Informal institutions**: In some cases, actors may opt for more informal, non-binding and flexible arrangements, which are not based neither on formal treaties nor on contracts. Informal institutions can be intergovernmental, like the well-known Wassenaar Arrangement, or multistakeholder integrating combinations of state and non-state actors, like the Paris Call for Trust and Security in Cyberspace.

The previous three categories – treaty-based, contract-based, and informal – are mutually exclusive (i.e. when the code 1 was assigned to one of them, the other two were coded as 0).

3.4 Membership

General membership information

a. **Name of members**: We include the names of an institution’s members when they are available in the member section of its website. In some cases, the websites of our institutions only mention the number of members they have, but they do not provide a full list. This omission may be owed to the large membership of the institution (for example, DIGITALEUROPE’s membership includes 35.000 companies) or to the institution’s confidentiality policy[14].

   - Note that any sub-divisions of members into further categories (e.g. platinum, gold, silver, or blue) according to the amount of their financial contributions has not been taken into account.

[14] For example, the Anti-Phishing Working Group mentions that “because electronic crime is a sensitive subject, the APWG maintains a policy of confidentiality of member organizations” https://apwg.org/membership/

- We have included only full members but excluded observers, participants, sponsors, affiliate members and suspended members.

b. **Number of members** (count variable):

- In most cases, the number of members is readily available in the membership section of the institution's website.
- In the absence of such a number, we have manually counted the members listed in the membership section.
- In rare cases, there was neither a number nor a list of members.

c. **Regional / Transcontinental:** In order to differentiate between institutions with a regional scope and those that are transcontinental, we have adopted the UN's division of regions which recognizes 6 major areas: Africa; Asia; Europe; Latin America and the Caribbean; Northern America, and Oceania. The institutions whose members are located in two or more countries from the same region/continent have been designated as regional (assigned the code 1). Those whose members are located in two or more countries that belong to different regions have been designated as transcontinental (assigned the code 1). Note that these two variables are mutually exclusive, namely when 1 was assigned to one of them the other was coded as 0.

Membership type

a. **Governmental members**: In this category we include both governments and sub-state bodies and authorities, like national law enforcement agencies, national standardization bodies and national regulatory authorities. Also, we include central banks (we have felt comfortable to do so because the Bank for International Settlements whose members are central banks is included in latest CoW IGO data set version 3.0).

b. **Business**: Privately-owned for-profit companies regardless of their size (for example, software developers, anti-virus vendors, network operators, security providers, equipment and device makers, internet service providers, technology companies etc.).

c. **Individuals**: In this category we include experts who act in their professional capacity and do not depend on or represent any government (for example, technical experts, engineers, computer security experts, trademark professionals and scholars).

d. **Non-profit organizations**: In this category we include academic institutions and non-governmental organizations.

e. **Incidence response teams**: In this category we include both computer emergency response teams (CERTs) and computer security incidence response teams (CSIRTs) that coordinate responses to cyberattacks, report incidents and educate the public about Internet security. These teams may be publicly-run, some are private and others involve public-private cooperation.[15]

f. **Intelligence services**: We decided to create a separate category for intelligence agencies instead of including them in governmental members because we consider that cooperation among them is not as ordinary as cooperation among other sub-state authorities and bodies. Also, there are few examples of institutions whose members are intelligence

[15] For more info on CERTs and CSIRTs, see DeNardis, 2014, pp. 91-92.

Funded by the Horizon 2020 Framework Programme of the European Union. Grant agreement number 822654

agencies in our sample and we can capture them easily and set them apart for the moment.

g. **Formal intergovernmental organizations**: Only includes the cases in which FIGOs appear directly as members of an institution, not through their members.

h. **Business associations**: These organizations can be global or national and they are created and funded by businesses that operate in a specific sector or industry. Their functions can vary, but they usually focus on connecting their members, they provide information and training, and engage in lobbying activities.

For variables a-h above, the code 1 was assigned to them when an institution had members of that specific membership type and a 0 when it did not have any of that type. Note that these variables are not mutually exclusive, as any given institution may integrate many different types of members.

3.5 Governance functions

a. **Norm-setting**: Both public and private initiatives that contribute to the development of cybernorms (we use Katzenstein's standard definition of norms as: collective expectations for the proper behaviour of actors with a given identity). Therefore, both the adoption of legal documents and the promotion of principles and best practices by private actors are included in this category.

b. **Technical standard-setting**: Development of technical specifications, standards and protocols (including standards and guidelines for testing tools) that enhance the protection of industrial and critical infrastructure, as well as the security of online payments, privacy, data exchange and storage.

c. **Information-sharing**: Exchange of information and experiences among actors that contribute to cybersecurity. They can be technical information about malware, viruses and worms, warnings about known vulnerabilities and exposure to cyber risks or reports, guidelines and discussions about cyber risks and emerging cybersecurity trends.

d. **Intelligence-sharing**: It is a form of information-sharing, but it concerns information that is by definition more exclusive, sensitive and confidential in nature. It is often distributed through the more secretive channels of national intelligence services, but it can also be shared among other types of actors.

e. **Agenda-setting**: encompasses the creation of documents and reports that aim to inform policy-making (e.g. policy-briefs and risk analyses), as well as lobbying activities that aim to put the interests of a specific community or industrial sector on the global governance agenda.

f. **Capacity-building**: This category includes a wide range of activities and initiatives (including the publication of guidelines, the organization of conferences, specialized courses, workshops and training programmes) that aim to train incidence response teams and strengthen the capacity of cybersecurity experts to identify and respond to cyberthreats.

g. **Hard / soft functions**: Governance functions were grouped into two categories. Norm-setting, technical standard-setting and intelligence-sharing are considered as hard functions, while information-sharing, agenda-setting and capacity-building have been coded as soft functions.

For variables a-g above, the code 1 was assigned to them when an institution performs that specific type of governance function and a 0 when it does not. Note that these variables are not mutually exclusive, as any given institution may perform many different functions.

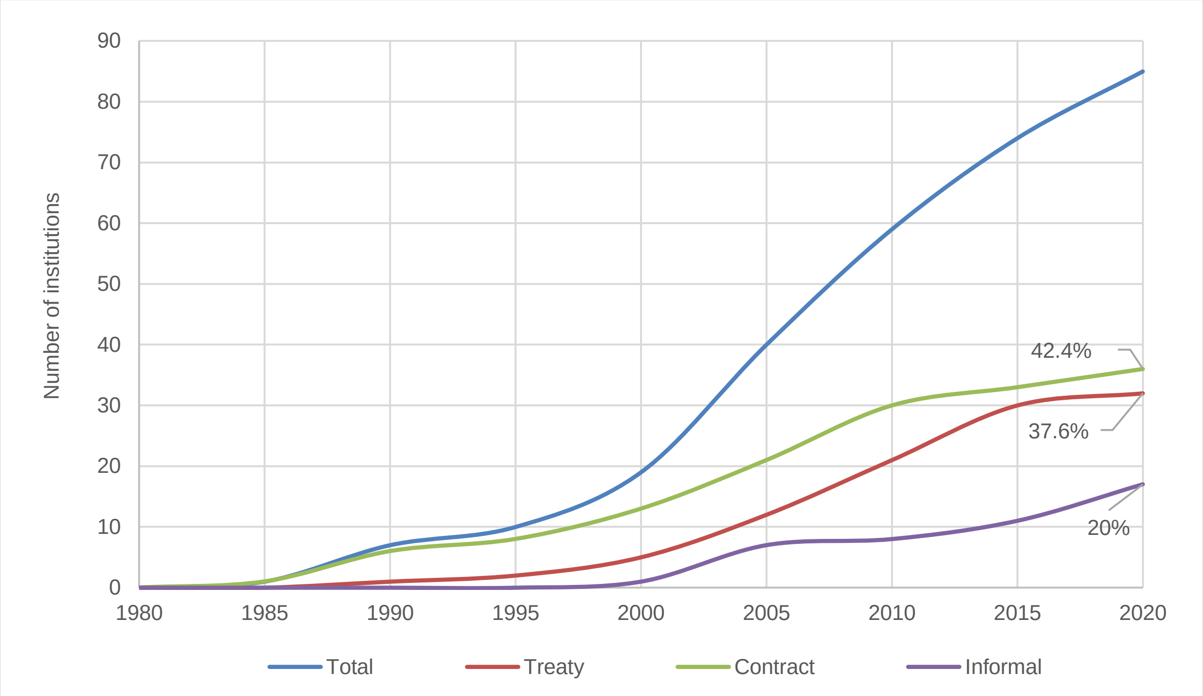
4. Descriptive analysis of data

With cybersecurity being a relatively new issue and gaining traction on the global governance agenda only in recent decades (see also section 2), it is one of the newest regime complexes. In this section, we begin by providing an overview of this novel regime complex, studying both the present configuration of its institutions and the evolution of the complex. We then present two key findings on the regime complex, regarding the scope of action of the institutions and the prevalence of the multistakeholder model.

4.1 Overview of the regime complex for global cybersecurity governance

Even though the first efforts to promote cybersecurity can be traced back to the 1980s,[16] the real expansion and **development** of the regime complex for global cybersecurity governance has mostly occurred over the past twenty years. To be more precise, almost 80% of the institutions began their work on cybersecurity governance after 2000[17] (see figure 1).

Figure 1 Years of involvement in cybersecurity governance depending on institutional form



Contract-based institutions (42.4% of all institutions in our database) were by far the earliest contributors to cybersecurity: a full third of them were created or started to engage in activities that promote cybersecurity before 2000, mostly through the creation of technical standards and protocols for information and data security. By contrast, treaty-based institutions (37.6%

[16] For example, the International Federation for Information Processing set up its Technical Committee 11 on Security and Privacy Protection in Information Processing Systems as early as 1983 and the well-known ISO/IEC Joint Technical Commission on Information Security and Cybersecurity was created in 1989.
[17] For those institutions that work solely on cybersecurity issues, the year of creation was used here; for those institutions that work on multiple issue areas, the year they became involved in cybersecurity was used (see also section 3.2 and Annex 3).

Funded by the Horizon 2020 Framework Programme of the European Union. Grant agreement number 822654

of the institutions) were slower to react to cyber threats. Almost 85% of them became involved in cybersecurity governance over the past two decades. Finally, informal institutions (20% of the institutions in our database) are clearly the late-comers: only one of them started to contribute to cybersecurity before 2000, while more than half did not do so until the beginning of the 2010s.

In terms of **geographic scope**, transcontinental cooperation is far more frequent (77.6%) in cybersecurity governance institutions than regional cooperation (22.4%). Interestingly, the regional institutions that participate in cybersecurity governance put great emphasis on the fight against cybercrime. As many as 84% of them have created specialized regional treaties on this issue or analyse data and exchange information about the activities of cybercriminals.

When it comes to size, 55% of our institutions have a relatively small number of **members** (less than 50). 19 of them have an average to big membership (50-200 members) and only 16 of the 85 (19%) institutions have a membership size that exceeds the 200-member mark (Internet Society, for example, has nearly 70,000 members, and the International Trademark Association has 7000). With respect to the types of members that make up our institutions, governmental actors are by far the most common, followed by businesses and non-profit organizations (see figure 2). A limited number of institutions also integrate other stakeholders such as CSIRT/CERTs, business associations, individuals and intelligence agencies.

Figure 2 Types of members present in collective cybersecurity governance institutions

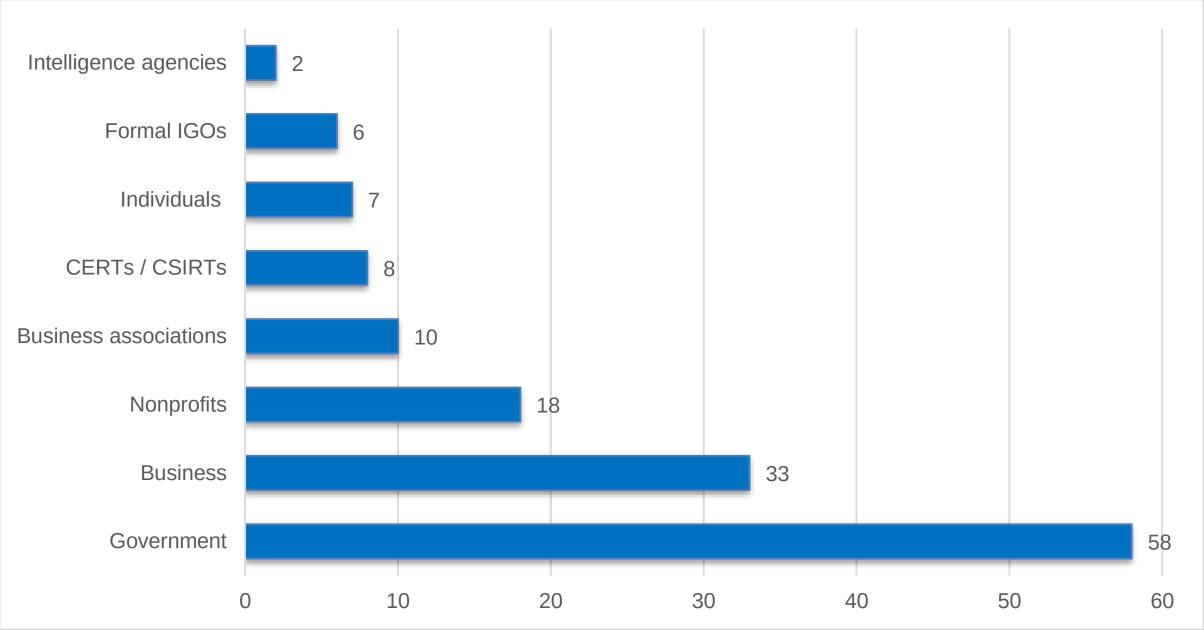
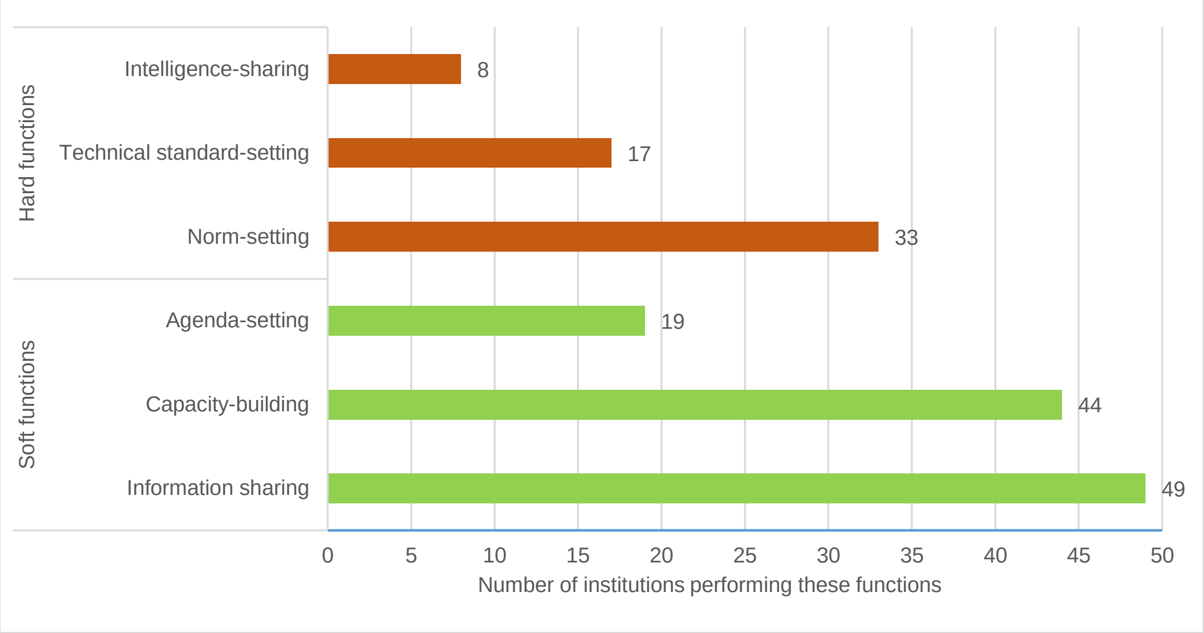


Figure 3 shows that information-sharing is the most common governance function, followed closely by capacity-building initiatives and cooperative efforts to develop cybernorms. Agenda-setting functions and the creation of technical standards are somewhat less common, while intelligence-sharing is the least common form of global cooperation in the promotion of cybersecurity.

Funded by the Horizon 2020 Framework Programme of the European Union. Grant agreement number 822654

Figure 3 Governance functions present in collective cybersecurity governance institutions



"Softer" governance functions – that is, tasks that require a looser cooperation and may therefore be easier to set up – are thus far more common that "harder" tasks, which generally call for more stable relations and broader consensus. To be more precise, more than half (54.7%) of all governance functions in our database engage in information-sharing and capacity-building. Even so, norm-setting is the third most common function, a rather significant observation considering how recent the area of cybersecurity governance is. Intelligence-sharing, finally, is the least common governance function. We can surmise that this may be related to the sensitive nature of this information; a great degree of trust is necessary between states holding such intelligence for these functions to take place. Another potential explanation is that intelligence services tend to remain outside of the public sphere by nature, meaning that they may be underrepresented in the dataset.

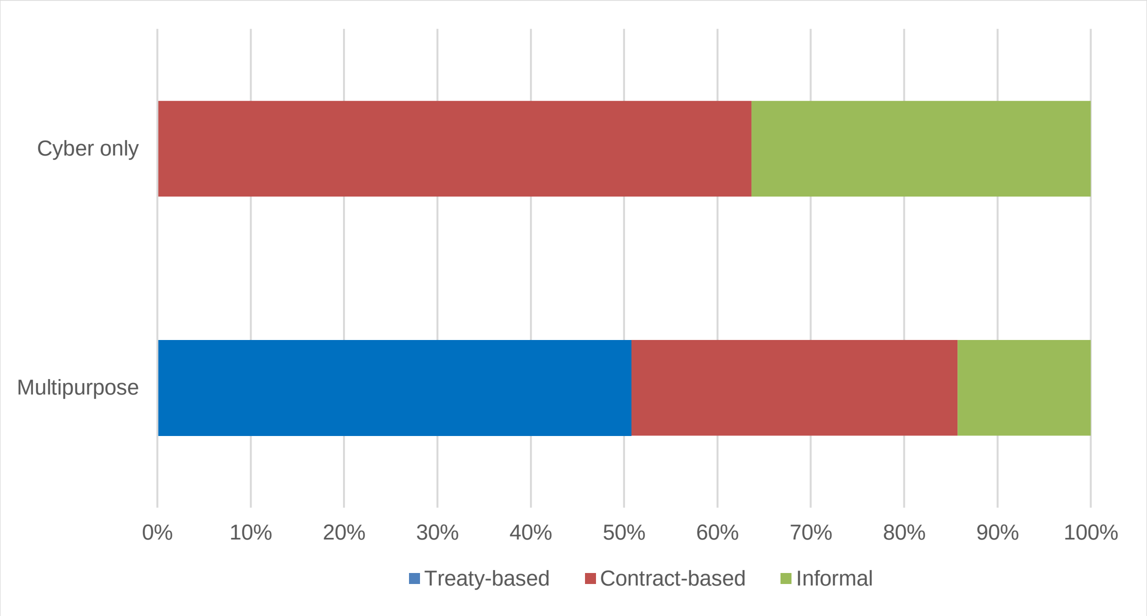
4.2 Institutions working on cybersecurity generally also work on other issue areas

Global governance institutions working on cybersecurity tend to focus not only on cybersecurity, but also on other topics: 74% of the institutions that contribute to cybersecurity also work on other issues of global governance, while only 26% of the institutions under consideration were created with the sole purpose of mitigating cybersecurity threats.

Cyber-only institutions emerged primarily after 2000 (this was the case for 18 out of 22 of them), at the same time as cybersecurity threats were rising on the agenda. Similarly, among the "multipurpose" institutions, 78% became involved in cybersecurity only after 2000 – but fully 22% (14 out of 63) saw cybersecurity governance added to their portfolios earlier. As such, multipurpose institutions account for 78% of all cybersecurity governance institutions created before 2000 (14 of 18).

Interestingly, there is not a single treaty-based institution that works solely on cybersecurity. 64% of all cyber-only institutions are contract-based and 36% are informal. The picture is very different among multipurpose institutions, where more than half are treaty-based (32 of 63), 22 contract-based, and 9 informal (see figure 4).

Figure 4 Institutional design of multipurpose and cyber-only institutions



As one might expect, institutions that focus only on cybersecurity are in most cases highly specialized, often managing concrete technical challenges (anti-phishing, anti-malware, anti-virus or unsolicited communications), coordinating computer emergency response teams or exchanging information on cybercrime. For example, the Anti-Phishing Working Group is a well-known international consortium that brings together businesses that have fallen victims to phishing, security services companies, trade associations, law enforcement agencies, regional IGOs and government agencies in order to provide a unified global response to cybercrime and promote public awareness. By contrast, multipurpose institutions are, in most cases, either well-established intergovernmental organizations (the United Nations, for example, was created in 1945 and became involved in cybersecurity governance in 1998) or highly technical organizations that have regulated several other aspects of telecommunications (The European Committee for Standardization, for instance, was created in 1961 and began working on cybersecurity in 2003) for decades.

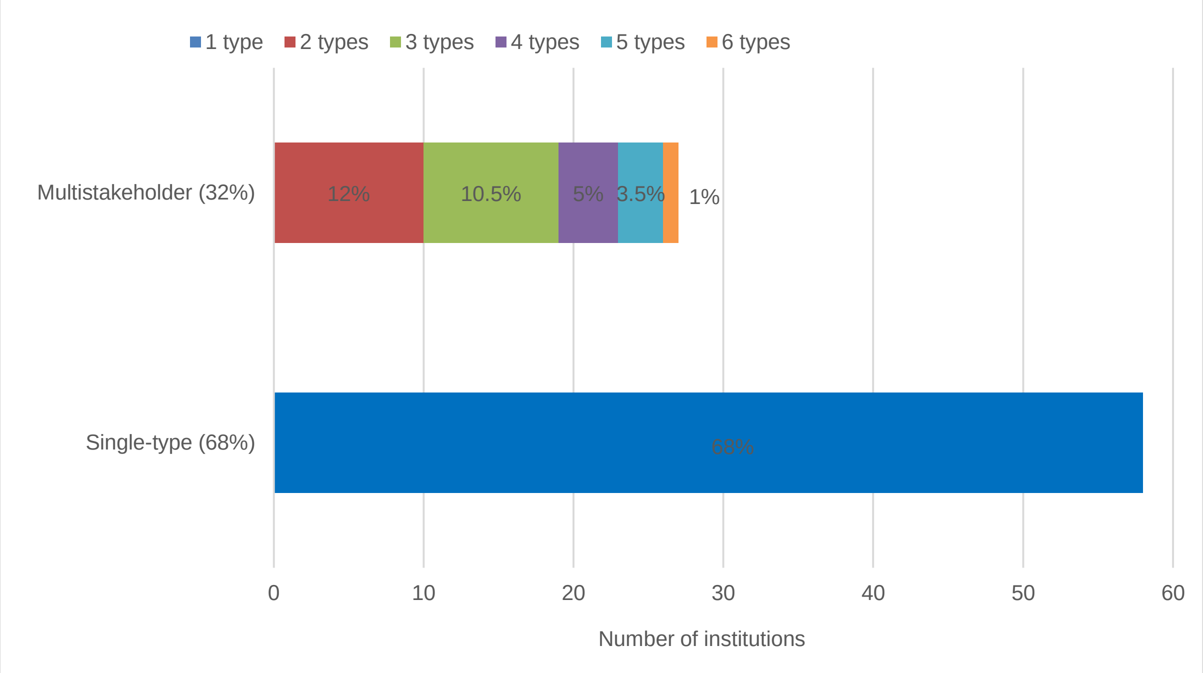
In conclusion, it appears that stakeholders who participate in cybersecurity governance generally prefer to **graft** their governance initiatives onto pre-existing institutions instead of creating new ones. This tendency is understandable if we take into consideration the advantages of grafting, including the reduction of costs and time for negotiations, as well as the sense of legitimacy that surrounds the grafted initiatives when the institution is well-resourced and visible (Finnemore & Hollis, 2016, p. 446). It also fits the bounded rationality model of institutional choice outlined by Jupille et al. (2013), which suggests that satisficing behaviour will lead actors to "take smaller [institutional] steps" (p. 7), such as using an existing institution, to address a cooperation problem, rather than opting for "costlier and riskier strategies" (p. 19), such as creating a new institution.

4.3 Is the multistakeholder model of internet governance replicated in cybersecurity governance?

Single-membership-type organizations outweigh multistakeholder institutions

Over two thirds (68%) of the institutions in the cybersecurity regime complex are composed of a single type of members, as shown in figure 5. This configuration stands in contrast with the multistakeholder nature highlighted in the most common definition of Internet governance: “the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet” (WGIG, 2005, p. 4) (see also section 2).

Figure 5 Number of member types per institution



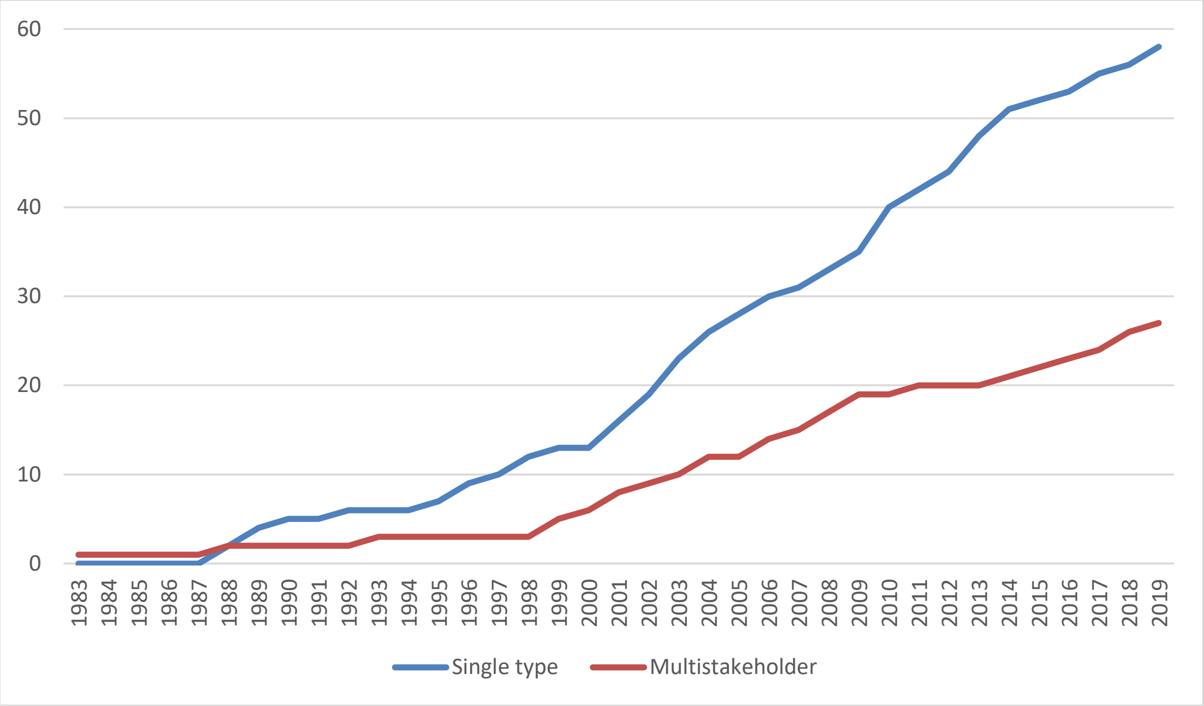
Our data therefore reveals that the regime complex related to cybersecurity may differ from Internet governance in this sense. Nevertheless, multistakeholderism is not absent from cybersecurity governance. Fully 32% of the global cybersecurity institutions are of a multistakeholder nature, and over half of those institutions (52%) were either created or commenced their work on cybersecurity during the 2000s. This timing correlates to some degree to the push towards multistakeholderism in Internet governance in the 2000s.

A notable switch, however, took place at the end of that same decade, affecting the regime complex and its evolution. The large-scale cyberattacks against Estonia and the Stuxnet virus in the late 2000s inaugurated an era of state-sponsored cyberattacks that diverted attention from inclusiveness towards national security narratives of protecting critical infrastructures and the state’s economic well-being from cyber threats (van Eeten, 2017, p. 429). The evolution of the cybersecurity regime complex reflects this turning point. As shown in figure 6, while some multistakeholder institutions continued to be created after 2010, their growth rate started

Funded by the Horizon 2020 Framework
Programme of the European Union.
Grant agreement number 822654

to taper. Institutions composed of a single type of member, on the contrary, continued to show strong growth after 2010.

Figure 6 Multistakeholder and single membership type institutions and their year of involvement in cybersecurity



The role of institutions comprising governmental members only

Within the group of institutions whose members are of one type only, nearly two-thirds (64%) comprise only governmental actors (22% are made up of businesses, and the remaining 14% are composed of other actors such as individuals, CERTs or intelligence services). Cybersecurity, in other words, remains an issue of clear concern for states, and they often address its governance directly in cooperation with other states. Interestingly, this is also reflected in the governance of such institutions: 76% of the government-only organizations are treaty-based.

In any case, states also participate in cybersecurity governance institutions with more diverse membership. In fact, nearly four-fifths (78%) of all multistakeholder institutions also include governmental actors. In terms of governance functions, institutions composed solely of governmental members are twice as likely as multistakeholder institutions to engage in norm-setting.

Funded by the Horizon 2020 Framework Programme of the European Union. Grant agreement number 822654

5. Discussion

In this paper, we set out to systematically study the global governance of cybersecurity, one of the newest regime complexes in existence: nearly 80% of the institutions in the complex began their work on this issue after 2000. In order to capture this rapidly evolving field, we created a novel dataset of 85 institutions, which represents, to our knowledge, the most up-to-date map of this regime complex. In addition, the data collected goes beyond previous mapping exercises by focusing on membership, scope, institutional design and governance functions.

The general shape of the regime complex is the following: 85 treaty-based, contract-based and informal institutions populate a field where governmental actors are highly present, as members of over two thirds of the institutions. In general, the institutions are relatively small in terms of membership size (the majority have fewer than 50 members); however, there are few outliers with tens of thousands of members. Soft governance functions such as information-sharing and capacity-building are more common than hard ones, but norm-setting (a hard function) is also quite common. Finally, the regime complex displays a clear evolution, with contract-based institutions populating the field first (some of them even before 2000), followed by treaty-based institutions, and informal institutions in the most recent decade of the 2000s.

Three main findings stand out from our research. First, there appears to be a tendency to govern issues of cybersecurity from existing global governance institutions rather than to create new ones to exercise these functions. This matches traditional institutional views that point to the high transaction costs involved in the creation of a new institution when positing that when a novel governance need arises, states are more likely to add new functions to existing institutions than to create a new one (Duffield, 2003, p. 418). Our data confirm that three fourths of the institutions working on cybersecurity also work on other issue areas. Interestingly, among the institutions that were created to work solely on cybersecurity – which tend to be very specialized, focusing on concrete technical challenges, there is not a single treaty-based institution: instead, ‘cyber only’ institutions are mainly contract-based and sometimes informal.

Second, the multistakeholder model of internet governance is only partially replicated in cybersecurity governance. Institutions containing multiple types of members did take off in cybersecurity governance in the 2000s, precisely when the multistakeholder model of internet governance was highlighted by the UN’s Working Group on Internet Governance. There is a clear turning point in the cybersecurity regime complex, however, when cybersecurity would appear to diverge from this model. After a spate of state-sponsored cyberattacks in the late 2000s, single membership-type organizations continue to grow strongly, while the entry rate of multistakeholder institutions slows.

This point is related to our third finding: governmental actors remain highly present in the regime complex. While businesses are also clearly involved in the regime complex (as members of nearly forty percent of the institutions), governmental actors are far more widespread still: they participate in two thirds of the institutions in the regime complex, are members of four fifths of the multistakeholder institutions, and make up the clear majority of single membership-type organizations as well. Although the Internet itself – and its original governance – were founded in the private sphere, governments have clearly taken on cybersecurity as a concern to be addressed through global governance. They do so both in direct cooperation with other states and in multistakeholder settings.

The present study opens doors to further research. For one, it may be enlightening to extend the dataset to include bilateral institutions as well, as the current dataset is limited to those institutions containing at least three members. In addition, regional cooperation was found in our study to be far less prevalent than transcontinental cooperation. It may be worthwhile to investigate which subareas of cybersecurity are dealt with in regional contexts, and which in transcontinental cooperation, given that the dataset currently does not contain data on subareas and outputs of the institutions. Another avenue of research is to apply case studies in order to add a qualitative level of depth when investigating, for instance, the why and in which cases actors choose to address cybersecurity through existing organizations rather than create new ones. The data collected could also be further expanded to allow for a social network analysis of members and institutions, and thus explore clusters and centralities in the regime complex. Finally, this research has not delved into the question of the effectiveness of the regime complex: is the proliferation of institutions in this field contributing to an increased degree of cybersecurity?

Bibliography

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

Christou, G. (Spring/Summer, 2017). *EU-Japan security cooperation: Challenges and opportunities - the EU's approach to cybersecurity*. https://core.ac.uk/download/pdf/83927508.pdf

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

DeNardis, L. (2020). *The Internet in everything*. Yale University Press.

Dunn Cavelty, M. (2008). *Cyber-security and threat politics*. Routledge. https://doi.org/10.4324/9780203937419

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894

Georgieva, I. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy*, *41*(1), 33–54. https://doi.org/10.1080/13523260.2019.1677389

Green, J. F., & Auld, G. (2017). Unbundling the regime complex: The effects of private authority. *Transnational Environmental Law*, *6*(2), 259–284. https://doi.org/10.1017/S2047102516000121

Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: Finding the governance in Internet governance. *New Media and Society*, *19*(9), 1406–1423. https://doi.org/10.1177/1461444816639975

Jupille, J., Mattli, W., & Snidal, D. (2013). *Institutional choice and global commerce*. Cambridge University Press.

Keohane, R. O., & Nye, J. S. (2000). Governance in a globalizing world. In J. S. Nye & J. D. Donahue (Eds.), *Governance in a globalizing world* (pp. 1–41). Brookings Institution Press.

Keohane, R. O., & Victor, D. G. (2011). The regime complex for climate change. *Perspectives on Politics*, *9*(1), 7–23. https://doi.org/10.1017/S1537592710004068

Kleinwächter, W. (2004). Beyond ICANN vs ITU? How WSIS tries to enter the new territory of Internet governance. *Gazette: The International Journal for Communication Studies*, *66*(3–4), 233–251. https://doi.org/10.1177/0016549204043609

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*, *19*(6), 466–492. https://doi.org/10.1108/DPRG-05-2017-0024

Morgan, S. (2019). *2019 Official annual cybercrime report next two decades*.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. The MIT Press.

Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415–428. https://doi.org/10.1108/DPRG-05-2017-0025

Mueller, M., & Kuerbis, B. (2014). Towards global Internet governance: How to end U.S. control of ICANN without sacrificing stability, freedom or accountability. In *SSRN Electronic Journal* (2014 TPRC Conference Paper). https://doi.org/10.2139/ssrn.2408226

Nye, J. S. (2014). The regime complex for managing global cyber activities. In *Global Commission on Internet Governance Paper Series 1* (1, Issue 1).

Olson, M. (1965). *The logic of collective action: Public goods and the theory of groups*. Harvard University Press.

Pevehouse, J., Nordstrom, T., McManus, R., & Anne Spencer Jamison. (2020). Tracking organizations in the world: The Correlates of War IGO Version 3.0 datasets. *Journal of Peace Research*, *57*(3), 492–503.

Portnoy, M., & Goodman, S. (2009). *Global initiatives to secure cyberspace: An emerging landscape*. Springer Science and Business Media, LLC. https://doi.org/10.1017/CBO9781107415324.004

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Oxford University Press. https://doi.org/10.5860/choice.188472

Solms, R. Von, & Niekerk, J. Van. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance, 19*(6), 429–448. https://doi.org/10.1108/DPRG-05-2017-0029

WGIG. (2005). *Report of the Working Group on Internet Governance*. https://www.wgig.org/docs/WGIGREPORT.pdf

Zittrain, J. (2008). *The future of the Internet and how to stop it*. Yale University Press.

Annex 1: Cybersecurity governance in the European Union

While computer crime and information security were recognized as important issues by the European Community as early as the late 1970s (Christou, 2018, p. 357), it was not until very recently that the European Union started to treat cybersecurity as an area of concern in its own right. Prior to 2007, cyber policies in the EU were dispersed across different Regulations and Directives, key dimensions were missing and the coordination required for the construction of an effective security ecosystem around cybersecurity was lacking (Christou, 2017, p. 2).

This situation started to change quickly after the large-scale cyberattacks against Estonia, Lithuania and Georgia and the breaks of transcontinental cables in 2008 (European Commission, 2009). These events served as a wake-up call and led to landmark developments in 2013. During that year, "the European Commission released its Cybersecurity Strategy, entitled 'An Open, Safe and Secure Cyberspace', paired with the proposal for a Directive (the NIS Directive). Also in 2013, the European Cybercrime Center (EC3) at Europol commenced its activities" (Dunn Cavelty, 2018, p. 313).

With its Cybersecurity Strategy, the European Commission attempted to bring together under a single framework three policy areas whose competencies mandates were previously clearly separate: the Digital Agenda, law enforcement and, defence, security and foreign policy (Robinson, Horvath, Cave, & Roosendaal, 2013). Notably, the document articulated five strategic priorities to manage cybersecurity challenges as well as the key actors who would bear the responsibility of promoting these objectives.

The first priority refers to a set of measures that can increase network and information security and promote cyber resilience in support of Critical Information Infrastructure Protection (CIIP). To enhance the capacity of both the public and private sectors to prevent, detect and respond to cybersecurity incidents, the Commission asked the European Network and Information Security Agency (ENISA) to assist all EU member states in the development of strong national cyber resilience capabilities (European Commission, 2013, p. 7).

The second major pillar is the fight against cybercrime. In addition to urging all member states to transpose and implement all directives related to cybercrime and ratifying the Council of Europe's Budapest Convention on Cybercrime, the Commission supported increased collaboration through the European Cybercrime Centre (EC3). Set up within Europol, the EC3 was entrusted with providing analysis and intelligence, facilitating cooperation and information-sharing, providing support to member states in cybercrime investigations and organising meetings with cybercrime experts (European Commission, 2013, p. 10).

In contrast to the first two objectives, the third area of cyber defence is the least developed. This is hardly surprising, since "the Common Security and Defence Policy (CSDP) remains the weakest link in the European integration project overall" (Dunn Cavelty, 2018, p. 9). The EU's strategic priorities and actors have been laid out in the "EU Cyber Defense Policy Priorities" adopted by the European Council in 2014 (and updated in 2018). Cyber defence was further reinforced in 2017, thanks to Council's adoption of a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, commonly referred to as the "Cyber

Diplomacy Toolbox". This Framework reaffirms the EU's commitment to settle international disputes in cyberspace by peaceful means, to encourage cooperation and facilitate the mitigation of threats. But perhaps more crucially, the Framework states clearly that a joint EU diplomatic response to malicious cyber activities may involve the use of measures within the Common Foreign and Security Policy, even restrictive ones –that is to say sanctions (Council of the European Union, 2017, p. 5).

The fourth priority of the EU is the development of industrial and technological resources for cybersecurity. In pursuance of this objective, the Digital Single Market Strategy presented in 2015 included an important public-private partnership (PPP) on cybersecurity. This partnership was signed in 2016 by the Commission and European Cyber Security Organization (ECSO) with the aim of stimulating European competitiveness and overcoming cybersecurity market fragmentation through innovation, building trust between member states and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions.

Finally, the fifth priority is a long-term aspiration of a more transversal nature. The EU will try to establish a coherent international cyberspace policy and promote its core values by mainstreaming cybersecurity issues into EU external relations and Common Foreign and Security Policy and by establishing closer cooperation with other intergovernmental organizations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS.

Annex 2: List of institutions in the dataset

3rd Generation Partnership Project
African Network Operators Group
African Union
Alianza contra Piratería de Televisión Paga
Anti-Counterfeiting Trade Agreement
Anti-Malware Testing Standards Organization
Anti-Phishing Working Group
Asia Pacific Computer Emergency Response Team
Asia-Pacific Economic Cooperation
Asia-Pacific Telecommunity
Association of Southeast Asian Nations
Bank for International Settlements
Caribbean Community and Common Market
Cloud Security Alliance
Club de Berne
Common Market for Eastern and Southern Africa
Commonwealth of Independent States
Commonwealth Telecommunications Organisation
Computer & Communications Industry Association
Council of Europe
Cyber Threat Alliance
DIGITALEUROPE
DNS-Operations and Research Center
East African Community
Economic Community of Central African States
Economic Community of West African States
Eurasia Network Operators Group
European Central Bank
European Committee for Standardization
European Cyber Security Organisation
European Digital Rights
European Law Enforcement Organisation
European Telecommunications Standards Institute
European Union
European Union Agency for Cybersecurity
Financial Action Task Force
Financial Stability Board
Five Eyes Alliance (AU, CA, NZ, US, UK)
Forum for Incident Response and Security Teams
Group of 7
Groupe Speciale Mobile Association
Industrial Internet Consortium
Institute of Electrical and Electronics Engineers
International Chamber of Commerce
International Criminal Police Organisation

Funded by the Horizon 2020 Framework Programme of the European Union. Grant agreement number 822654

International Electrotechnical Commission
International Federation for Information Processing
International Monetary Fund
International Organization for Standardization
International Telecommunication Union
International Trademark Association
International Watch and Warning Network
Internet Engineering Task Force
Internet Infrastructure Coalition
Internet Society
IoT Security Policy Platform
League of Arab States
London Action Plan / Unsolicited Communications Enforcement Network
Messaging, Malware and Mobile Anti-Abuse Working Group
Microsoft Cybersecurity Tech Accord
Microsoft Virus Information Alliance
NATO Cooperative Cyber Defence Centre of Excellence
North Atlantic Treaty Organization
Organisation for Economic Co-operation and Development
Organisation of Islamic Cooperation
Organization for Security and Co-operation in Europe
Organization for the Advancement of Structured Information Standards
Organization of American States
Paris Call for Trust and Security in Cyberspace
Payment Card Industry Security Standards Council
Shanghai Cooperation Organisation
Siemens Charter of Trust
Society for the Policing of Cyberspace
Southern African Development Community
Spamhaus Project
The Commonwealth of Nations
The Software Alliance
Trilateral Cooperation Secretariat
United Nations
Wassenaar Arrangement
Wi-Fi Alliance
World Customs Organization
World Economic Forum
World Intellectual Property Organization
World Wide Web Consortium

Annex 3: Sources used to populate the dataset

1. A working paper by **Joseph Nye (2014)** for the Global Commission on Internet Governance.[18] This influential and commonly cited piece maps a large number of institutions that participate in cybergovernance. Although the author admits that his list of institutions is “deliberately incomplete” (Nye, 2014, p. 7), it is a valuable source because he uses a regime complex approach that encompasses actors and institutions from many different regimes (trade, finance, intelligence, intellectual property, human rights, telecom, technical standards etc).

2. A 2009 book by **Michael Portnoy and Seymour Goodman**, which contains the most comprehensive study of governance enterprises aimed at promoting security in cyberspace (Portnoy & Goodman, 2009). The authors offer an exhaustive compilation of initiatives undertaken at the global and regional level by both intergovernmental and non-governmental organizations. Even though the policy area has developed vertiginously since the book was written and some initiatives have ceased to exist, its presentation of specific contributions to cybersecurity governance remains valuable and relevant.

3. An article by **Brenden Kuerbis and Farzaneh Badiei’s** (2017), which relies on the institutional economics concept of governance structures to survey and describe the market, network and hierarchy activity, in order to illustrate how they interact to govern cybersecurity (Kuerbis & Badiei, 2017).

4. The **Geneva Internet Platform** (GIP) webpage, in particular, the “actors” sub-section of the “resources” section at the GIP Digital Watch Observatory. In order to select only those actors working cybersecurity and not Internet governance in general, a series of filters were used to narrow down the search: Cyberconflict and warfare, Cybercrime and Network Security, Telecommunications Infrastructure, Intellectual Property Rights, Encryption, Digital Standards, Critical Infrastructure, Cloud Computing, E-commerce and Trade.

5. The **Cyber Policy Portal created by the United Nations Institute for Disarmament Research**. This portal offers two sources for data collection: on the one hand, the “Organizations” section includes information about intergovernmental organizations and their cyber-related agencies, initiatives and subsidiary bodies; on the other hand, the “Multilateral Frameworks” section includes information about public, private and multistakeholder norm-setting initiatives.

The number of cases extracted from our five sources were: Nye: 51, Portnoy and Goodman: 72, Kuerbis and Badiei: 37, Geneva Internet Platform: 151, Cyber Policy Portal: 37. Of course, many of the institutions were mentioned in more than one source, and therefore, the number of our case population is not equivalent to the sum of cases found in the five sources. Overall, the distribution of cases was the following: 198 institutions appeared in one source, 37 were mentioned in two sources, 18 in three sources and 5 in four sources. The high number of

[18] The Global Commission on Internet Governance was a two-year joint initiative by the Centre for International Governance Innovation and Chatham House. It was launched at the World Economic Forum in 2014 with the objective of articulating and advancing a strategic vision for the future of internet governance.

Funded by the Horizon 2020 Framework Programme of the European Union.
Grant agreement number 822654

institutions appearing in only one of the sources is owed to the different approaches and definitions of governance, actors and cybersecurity employed in the five sources.

Annex 4: Year of involvement - Data collection protocol

1. Data was collected only for the 63 institutions that are active in multiple issue areas of global governance. For the 22 single-issue institutions in our data set, their year of creation is, naturally, the year they became involved in cybersecurity governance.

2. In order to identify the year that these institutions started to contribute to cybersecurity governance, only the following concrete commitments and outputs have been taken into account:
   a. Publishing of strategies, agendas, declarations, statements, communications
   b. Creation of specialized forums, technical committees, task forces, working groups / expert groups
   c. Adoption of model laws, treaties, conventions, and agreements
   d. Issuing of guidelines, best practices, working papers, policy documents, reports with policy recommendations, white papers
   e. Adoption of resolutions and decisions
   f. Creation of information-sharing networks
   g. Creation of technical standards, protocols, and specifications
   h. Imposition of export controls
   i. Organization of workshops and conferences

   In contrast, the following outputs have *not* been taken into account:

   a. **Vague calls to action that do not establish concrete obligations.** For example, cyber defence became part of NATO political agenda at the Prague Summit in 2002 for the first time. However, the Prague Summit Declaration only offers a vague goal of strengthening the capabilities of member states to defend against cyberattacks without establishing concrete goals or offering a roadmap. According to these considerations, NATO's involvement in cybersecurity did not occur in 2002, but rather when the organization approved its first Policy on Cyber Defence in 2008.
   b. **Preliminary actions and requests that culminate with the adoption of binding legal instruments**. For example, the process of harmonising the cybersecurity legal frameworks of Central African states commenced at a workshop organized in 2011, at the request of the Ministers in charge of Telecommunications and ICTs of ECCAS member states. However, the model laws were not adopted until 2016.
   c. **Draft treaties**
   d. **Requests for drafts**. For example, the initiative for the creation of the Model Law on Computer and Computer-Related Crime came from Commonwealth Law Ministers at a meeting held in 1999 and an expert group meeting was convened by the Commonwealth Secretariat in 2000 to prepare drafting instructions for a model law on computer and computer related crime. But the final draft and its adoption were finalized in 2002.
   e. **Unpublished outputs**. For example, as the IMF' staff has become aware of the increasing importance of cyber risk, it has provided briefings to Management and has flagged cyber risk as a crucial issue since July 2016 in the (**unpublished**) regulatory updates provided periodically to the Board. However, its first working paper on cyber risk was only published in 2017.

3. Depending on the institutional design of each institution the availability of data differed greatly, so the data collection process was adapted accordingly:

   a. **Treaty-based institutions / Intergovernmental organizations (IGOs)**

      i. In order to find the year when IGOs expanded their scope to cybersecurity issues, data was collected from two online sources: the INCYDER database of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE: https://ccdcoe.org/library/incyder/) and UNIDIR´s Cyber Policy Portal (https://unidir.org/cpp/en/organizations). These databases have compiled all cybersecurity-relevant resolutions, declarations, communiqués, and treaties produced by several IGOs. When the IGOs included in our data set appeared in one or both of these databases, the year of the earliest output was taken as the year that the IGO started to work on cybersecurity. For example, according to INCYDER, the earliest evidence of the UN's interest in cybersecurity can be traced back to a 1998 Resolution of its General Assembly (A/RES/53/70) on the "Developments in the field of information and telecommunications in the context of international security". Therefore, 1998 was taken as the year that the UN started to work on cybersecurity.[19]

      ii. For the IGOs that did not appear in either of these databases, we consulted Portnoy and Goodman's (2009) book on Global initiatives to secure cyberspace. These authors collected information on the earliest contributions to cybersecurity for most of the institutions in the dataset.

      iii. For IGOs that did not appear in any of these sources, data was collected manually from their webpages. Once the type of contribution they made to cybersecurity was identified, we looked for information about the year that contribution was created in the "resources" section (filtering by date and issue-area) or in the descriptions of specific cybersecurity initiatives.

      iv. In the few cases where the output was a working group or a task force and the IGO did not contain information about the year it was established, information was retrieved from sources found on Google scholar.

      v. Tertiary sources like news pieces and workshop presentations were used only as a last resort or to confirm information found in other sources.

   b. **Contract-based institutions:**

      i. The main source for finding the year that contract-based institutions started to work on cybersecurity was the book "Global initiatives to secure cyberspace" by Portnoy and Goodman (2009). The authors collected information on the earliest contributions to cybersecurity for most of the institutions in the dataset.

      ii. For the institutions that did not appear in this book, information was retrieved from their webpages. When the outputs were written documents (i.e. working papers, white paper, policy analyses, briefings, guidelines, recommendations), they were available under the "resources" sections (or equivalent). After filtering

[19] Several IGOs have created legally binding treaties to address specific cybersecurity issues like cybercrime. Very often the creation of international treaties, from the phase of deliberations and negotiations to their final adoption, may be a long process. The moment when an IGO decided to work towards creating a treaty should logically count as the moment it started to take interest in cybersecurity. However, finding information about the preparatory phases is very challenging, as the idea for a treaty may appear during a workshop or be born at the request of a specific body, long before a draft is created. Moreover, a draft may be produced but not agreed upon and signed. Therefore, in the case of international treaties, we have taken the year of their final adoption as the year that the IGO started to work on cybersecurity.

by date and issues, the earliest output was taken as the year that the institutions started to contribute to governance.

iii. In some cases (DNS-OARC, Wi-Fi Alliance), the provision of cybersecurity appeared as one of the institution's core objectives. Therefore, the year of creation of these institutions coincides with year they started to work on cybersecurity.

iv. For institutions whose outputs were forums, technical committees, task forces, expert / working groups and their year of creation could not be found neither in Portnoy and Goodman (2009) nor in their websites, information was retrieved from sources found on Google scholar or other tertiary sources like news pieces, workshop presentations or curriculums of experts.

c. **Informal institutions**

i. For some well-known informal intergovernmental institutions like G7 or APEC, information about their earliest initiatives to contribute to cybersecurity was available in CCDCOE's INCYDER and Portnoy and Goodman's (2009) book.

ii. For the rest, information was retrieved from their websites. In the cases of the Wassenaar Arrangement and the Financial Stability Board, information was easily accessible, as their websites contain sections with their respective outputs that can be filtered by date.

iii. In the cases of AfNOG and ENOG, we consulted the resources available on their annual meetings (lists of workshops, presentations, and minutes) to determine when they touched upon issues of cybersecurity for the first time.

Funded by the Horizon 2020 Framework
Programme of the European Union.
Grant agreement number 822654