Cyber Sovereignty and Data Sovereignty

CSS CYBER DEFENSE PROJECT

Trend Analysis:

Cyber Sovereignty and Data Sovereignty

Zürich, November 2018

Version 2

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Authors: Marie Baezner, Patrice Robin

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zurich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zurich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching, Andreas Wenger, Director of the CSS

Please cite as: Baezner, Marie; Robin, Patrice (2018). Cyber sovereignty and Data sovereignty, Version 2, Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Objective and methods

The development of technology and cyberspace challenges traditional concepts of state boundaries and the principles of International Law. In its early days, the internet was said to be immune to sovereignty, and it was believed that freedom of speech would thrive as a result. It was assumed states would be kept at arm's length from internet governance. However, recent history has shown that state involvement in the development of cyberspace was ultimately inevitable. Sovereignty, a fundamental tenet of statehood, could not be simply ignored once it was clear the technology could be used for political gain.

Some economic actors have demanded greater cyber sovereignty to protect industrial and other economic sectors, assuming that cyber sovereignty is a form of autonomy in cyberspace. However, these demands demonstrate that the concept of sovereignty is still misunderstood or distorted from its definition in International Law. This Trend Analysis therefore seeks to shed light on the concept of cyber sovereignty by examining the ways in which states employ the concepts of sovereignty and cyber sovereignty in their national cybersecurity strategies. It then analyzes academic discussions of cyber sovereignty to establish whether a particular definition of this concept has become more prevalent than others. Finally, this Trend Analysis explores the historical development of the concept of sovereignty in other domains, such as sea, air and space, in order to compare it with the cyberspace domain.

Results

Empirical research on the use of the concepts of sovereignty and cyber sovereignty in national cybersecurity strategies revealed that only a minority of states used the term "sovereignty", and only one used the term "cyber sovereignty". The concept was primarily used by Western states, referring to a definition of sovereignty that closely matched the understanding described by International Law. States' cybersecurity strategies mostly displayed awareness that cyberattacks may constitute a threat to state sovereignty, or to re-emphasize that state sovereignty should be protected. To achieve this end, states planned to improve cybersecurity in the information technologies and networks of governmental, defense and critical infrastructures. This research revealed France as an exception; Paris referenced sovereignty most extensively throughout its national cybersecurity strategies. This difference may be explained by a specifically French historical and national understanding of the concept of sovereignty, as compared to the concept of state sovereignty in International Law.

A review of academic discussions on cyber sovereignty showed that academic debate mostly revolves around the application of the concept of state sovereignty in cyberspace. Scholars discuss rights and obligations tied to state sovereignty and how these might be applied in cyberspace. Researchers have also noted the physical dimension of sovereignty in cyberspace; physical infrastructures are necessary for the proper function of cyberspace, and most of those infrastructures are located on claimed territory. State sovereignty in cyberspace could therefore be seen as an extension of a state's territorial sovereignty. Academic discussions also revolve around the implications of state sovereignty in cyberspace, such as the definition of the use of force in cyberspace or the right to use cybertools in war.

Comparing the development of sovereignty norms in other domains showed that the discussion of the applicability of sovereignty in new situations evolved over a considerable time period. While previous sovereignty norms have developed in natural spaces considered as a global commons, cyberspace, which is man-made, might not be considered as a global commons. Overall, relevant discussions on sovereignty in other domains were similar to those regarding cyberspace, and showed that sovereignty issues in cyberspace will not be resolved overnight.

Finally, this Trend Analysis demonstrates that the most common understanding of cyber sovereignty is derived from its definition under International Law. It also shows that the European economic sector and French authorities lead an alternative debate on cyber sovereignty, which emphasizes strategic autonomy over traditional sovereignty. The concept of strategic autonomy is intrinsic to the wider protection of state sovereignty, and it consists of states maintaining control over data processing, data storage, and information technology infrastructures. As such, strategic autonomy and state sovereignty need to be differentiated.

Addendum

This updated version of the Trend Analysis on Cyber Sovereignty includes an addendum on data sovereignty. The purpose of the addendum is to analyze the concept of data sovereignty in detail, which was overlooked in the first version of the Trend Analysis. The concept of data sovereignty lacks a fixed definition but has been regularly used in politics, industries and law. This addendum defines data sovereignty as a state's ability to control data originating and passing through their territory.

The addendum examined national cybersecurity strategies to observe the use of the term "data sovereignty" in these documents. The research revealed that the term was not used in national strategies, but may be discussed at other political levels. After Edward Snowden's revelations on US mass surveillance of the

internet in June 2013, many states started to explore technical and legal ways to control data originating from and passing through their territories. Primarily, attempts were focused on 'tying' data to a specific territory. Proposed technical solutions included: the construction of a submarine internet cable between Latin America and Europe, bypassing the US; building a regional routing network; creating a national cloud computing service; and starting a national email service. These technical solutions were shown to be both inefficient and ineffective in preventing foreign surveillance of data. Technical experts reckon that data would be better protected with encryption than by tying data to a specific territory.

Nevertheless, the suggested technical and legal measures seem to miss the point of protecting data against foreign surveillance. To protect data originating in their territory, states should prioritize educating their population on ways to protect their personal data. States should also inform and raise awareness in the population about how businesses use their personal data. The analysis also suggested that the states with the most advanced data sovereignty policies are authoritarian. Democratic states that decide to strengthen their data sovereignty may expose themselves to criticism and risk unfavorable comparisons to these regimes.

Disclaimer

The documents used for this Trend Analysis are open-source. Many national cybersecurity strategies are openly accessible, but some states keep these documents confidential; these states, therefore, could not be included in the research. As a result, the empirical research may have been biased by this lack of universal access.

In addition, the documents studied in this Trend Analysis were written in English. This was desirable for methodological uniformity in the analysis, but there may be variations between the original documents and their English versions. An example of such a discrepancy was observed in the French 2015 national digital strategy, in which the word "sovereignty" in the French version was occasionally replaced by the words "digital strategic autonomy" in the English document.

1 Introduction

The development of cyberspace and technology has significantly changed the modern world, and prompted a re-evaluation of traditional International Law principles such as sovereignty. In its early days, the internet was governed by its users and believed to be immune to state sovereignty due to its interconnectedness and transnational nature (Franzese, 2009). However, as the number of internet users expanded across the world and its potential applications in the military and political domains became clear, states increasingly saw the benefit of possess at least some degree of sovereignty over virtual space. International discussions of the extent and applicability of state sovereignty to cyberspace came to replace the more idealistic views of the earlier era.

The role of state sovereignty in cyberspace has been widely discussed in academic literature. The United Nations Governmental Group of Experts[1] (UNGGE)[2] decided that International Law, including state sovereignty, was applicable in cyberspace (United Nations General Assembly, 2015). This decision implied that the Law of Armed Conflict was applicable in cyberspace, as well as all rights and obligations tied to principles of sovereignty. The Tallinn Manual on the International Law Applicable to Cyber Warfare and the Tallinn Manual 2.0, which discuss the status of the current International Law in reference to cyberspace, came to the same conclusion regarding state sovereignty in cyberspace (Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, 2017, 2013). Relevant literature mostly discusses how International Law principles can be applied in cyberspace and what challenges arise in this context (Jensen, 2015, 2011). The literature on sovereignty in cyberspace also analyzes the control that some states exercise over internet content, and the legal justifications for censorship based on principles of state sovereignty (Lotrionte, 2013; Maxey, 2017a). The fact that the majority of academic literature focuses on the legal implications of sovereignty in cyberspace indicates that the issue of cyber sovereignty is most often framed and understood as a matter of International Law.

Even though cyber sovereignty has been discussed at length in academic literature, it has not been consistently defined and remains vague. The definitions found in the literature range from an extension of the traditional understanding of International Law to cyberspace through to more diffuse concepts of control and independence. As definitions expand beyond the delineations of International Law, understandings often fail to view sovereignty as intrinsically linked to its associated legal rights and obligations. Moreover, this approach to defining cyber sovereignty - in terms of state control and independence in cyberspace - is a controversial one, as it may conflate issues of strategic autonomy with the separate concept of cyber sovereignty. While autonomy is highly relevant to state sovereignty, they are not synonymous.

This Trend Analysis suggests that how the concept of cyber sovereignty is applied needs to be examined in greater detail. Doing so can help avoid misunderstandings and ensure there is clarity in how policy-makers and academics use the term “cyber sovereignty” in their work.

The first part of this Trend Analysis proceeds as follows. Section 2 defines the concept of cyber sovereignty for the purposes of this document, in order to avoid any misunderstandings.

Section 3 examines national cybersecurity strategies to understand how policy-makers understand the terms “sovereignty” and “cyber sovereignty”. This analysis is based on a scan for these terms in national cybersecurity strategies. The results are then analyzed further to determine which types of states use these concepts, the frequency of their use, the context in which the concepts are used, and how the use of this term has changed over time.

In Section 4, the research looks at the major topics of academic debate regarding cyber sovereignty, identifying the ways in which academics approach cyber sovereignty, in which contexts, and the details they emphasize in their research.

Section 5 analyzes the evolution of the laws and norms of sovereignty in other domains, with an eye to compare previous discussions with the current debate regarding cyberspace.

Section 6 presents the general conclusions of this Trend Analysis and outlines the alternative debate revolving around the definition of cyber sovereignty in terms of state control and independence in cyberspace.

The second part of this Trend Analysis updates this document to include an addendum on data sovereignty. After the publication of the Trend Analysis on cyber sovereignty, it came to our attention that some economic actors and states had additional concerns regarding the financial impacts of controlling data through data sovereignty. To address this analysis gap, the addendum on data sovereignty was added to the overarching Trend Analysis on cyber sovereignty. The goal of this addendum is explicitly define data sovereignty and to analyze the usage of the term to better understand it.

The addendum proceeds as follows. Section 1 explores the various definitions of the term “data

[1] In 2004, the United Nations tasked a group of international experts to discuss the global cybersecurity agenda and the application of International Law in cyberspace. The group regularly publishes reports on the status of these issues (Digital Watch Observatory, 2017).

[2] Abbreviations are listed in Section 9.

sovereignty." Section 2 examines national cybersecurity strategies with the same methodology mentioned above, to analyze the use of the term "data sovereignty" by nation states. Section 3 analyzes the technical and legal solutions discussed by states to achieve data sovereignty. For each category, the addendum presents several potential solutions some states have employed, and examines the efficacy of their efforts to protect their data from foreign surveillance. Section 4 presents general conclusions from this addendum that can be applied to the broader Trend Analysis on cyber sovereignty, and suggests some measures on ways to improve data protection.

2 Definition of cyber sovereignty

While cyber sovereignty is a vague concept in general that is often used in relation to state power and independence in cyberspace, sovereignty itself is a clearly defined concept in International Law. Therefore, the concept of cyber sovereignty needs to be defined more precisely.

The concept of sovereignty goes back to the Peace of Westphalia of 1648, which established the Westphalian system of considering states to have sovereignty over their respective territories and domestic affairs, in which other states should not interfere (Franzese, 2009). The principle of sovereignty, which is inseparable from International Law, is also associated with the principle of equality, which implies that each state is equal under International Law and therefore has no power over other states (Jensen, 2015). Sovereignty is additionally one of the elements that constitute a state under International Law. Accordingly, a state, to exist as such, must have a population, a territory, effective political power and sovereignty (Daillier et al., 2009).

The principle of sovereignty entails rights and obligations. Rights are set on two levels: domestic and international. Domestic rights are derived from the fact that states may act as they wish within their territories: they are independent in their domestic actions. At the international level, this right consists of states' ability to represent their respective territories and populations in international forums. However, at the international level, state sovereignty must conform to principles of International Law, including decisions of the United Nations (UN) Security Council and the Law of Armed Conflict (Daillier et al., 2009; Jensen, 2015).

Obligations tied to sovereignty are composed of the obligation to recognize other states as sovereign, to refrain from intervening in other states' affairs, and to assume control over the actions of actors within a state's own territory (Daillier et al., 2009; Jensen, 2015).

Yet, the cross-border nature of cyberspace challenges state sovereignty and raises questions as to whether and how these principles of International Law can be applied to cyberspace. These questions will be examined in greater detail in Section 3, as they also form part of a wider academic debate.

In 2015, the UNGGE confirmed that states should respect International Law and sovereignty rights and obligations in their use of information and communications technologies, including in cyberspace (United Nations General Assembly, 2015). This implies that states should conform to the aforementioned rights and obligations in their activities in cyberspace. The UNGGE based its argument on the fact that cyberspace does not exist without physical infrastructures (e.g. servers and cables physically located on states' territories), and these infrastructures are subject to states' national jurisdictions (Kanuck, 2010).

Cyber sovereignty for the purposes of this Trend Analysis and within current academic debate is defined as the application of principles of state sovereignty to cyberspace.

Edward Snowden's 2013 revelations about the internet mass surveillance program of the US National Security Agency (NSA) revealed that technologies are vulnerable to other states' dominance in the domain of information and communication technologies. Vulnerabilities in both hardware and software do not merely constitute strictly technical vulnerabilities, but rather allow states to access information about another state's population and national security secrets. Snowden's revelations caused a loss of trust in these technologies and in US cyber-activities. The Snowden Affair started a wave of indignation and reflection among states on ways to protect what they called their cyber sovereignty. However, this use of the term cyber sovereignty is a misnomer. While it is true that state sovereignty was violated by these intrusions and massive espionage campaigns, it is necessary to differentiate between strategic autonomy issues related to cybersecurity and cyber sovereignty as defined by International Law. As will be discussed further in Section 6, the former concerns states' strategic ability to act autonomously at all levels of Grand Strategy, integrating military, economic, diplomatic and information resources, by building cyber capabilities based on trustworthy technologies. The latter, however, refers to the right to go to war and its legal implications.

3 Empirical observations

In this section, the study examines the definition of cyber sovereignty used by states in their national cybersecurity strategies. The research also looks at whether and how states employ the concepts of cyber sovereignty and sovereignty in general.

3.1 Scan of national cybersecurity strategies

The previous section defined the term cyber sovereignty as the application of state sovereignty rights and obligations to cyberspace. Given this definition, the aim was to see if states employed this term in their respective national cybersecurity strategies.

A total of 93 national cybersecurity and cyberdefense strategies[3] were scanned for the words "sovereignty" and "cyber sovereignty". This research focused exclusively on publicly available strategy documents published in English. Consequently, countries without national cybersecurity strategies, or countries that do not make their strategies publicly available or do not publish documents in English were not included in this research.

Open-source research using the International Telecommunication Union's (ITU) Global Cybersecurity Index (2017) and the ITU National Strategies Repository (2018) showed that 84 out of 193 countries worldwide had publicly available national cybersecurity strategies, and 69 states had their national strategies translated into English as per December 2017. In some cases, there were references to states having produced national cybersecurity strategies, but the relevant documents could not be located in open-source researches (e.g. Oman and Algeria).

The type of states that have national cybersecurity strategies are predominantly major powers and Western states, with the exception of some African, Arabic and South American states. Even though fewer than half of all states worldwide have a national cybersecurity strategy, this research was able to identify potential trends or patterns in the definition and use of the words "sovereignty" and "cyber sovereignty".

However, due to constraints of time and space, the research was restricted to searches for words rather than concepts, which might have limited its results. It is in fact possible that some states do not use the words "sovereignty" or "cyber sovereignty" in their national cybersecurity strategies but employ similar concepts. These would not have been included in the results but may have provided further insights into the understanding of sovereignty in cyberspace.

In addition to the scan for words, the research also looked at the type of states that used these words as well as at the contexts in which they were employed and the year the relevant strategy was published. In some cases, both current and older strategies of a single state were scanned to allow changes over time to be identified. For example, in the case of France, both the 2015 National Digital Security Strategy and the 2011 Information Systems Defence and Security were examined. These kinds of information further our understanding of how states understand and use the words "sovereignty" and "cyber sovereignty" and enable us to detect possible differences between states.

3.2 Results and analysis

The scan revealed that 18 out of 93 documents contained the word "sovereignty" and only one contained the term "cyber sovereignty".

Types of states

Out of 69 states with publicly available national cybersecurity strategies in English, only 15 states referred to the researched words. Half of the strategies containing the word "sovereignty" were from Western states, namely Canada, Finland, France, Hungary, Portugal, Spain, Australia and the UK, whereas the other half consisted of Chile, Colombia, Ghana, Japan, Nigeria, Russia and Saudi Arabia.

Canada was the only state to use the term "cyber sovereignty".

These results show that states use the concept of "sovereignty" in their national cybersecurity strategies relatively rarely. Based on the group of states that do use the term, it can be concluded that sovereignty in cybersecurity is mostly a Western concept, and Western states indeed tend to use the term more frequently than others. However, Western states are also over-represented in this group, as they account for a large portion of states that have published national cybersecurity strategies.

Frequency of use

Even though the words "sovereignty" and "cyber sovereignty" were found in these strategies, they were not used very often. On average, the word "sovereignty" was used twice in a document. Exceptions were noted in the strategies of Finland, Nigeria and Portugal, in which the word "sovereignty" was mentioned at least three times. However, one state, namely France, stood out in that it mentioned the word "sovereignty" nine times in

[3] A list of the countries selected for this scan is provided in Annex 1, Section 7.

its 2011 strategy and five times in its 2015 strategy. This particularity will be further discussed in subsection 3.4.

These results demonstrate that, while states use the word "sovereignty" in their national cybersecurity strategies, they rarely do so more than once in the document. This corroborates the previous finding that states tend to use the term infrequently in their strategies.

Context

The contexts in which the word "sovereignty" was used in strategies were various, but the word was never clearly defined in any of the documents. First, some states used the word in the context of states needing to protect the information systems of governments, defense forces and critical infrastructures in order to protect state sovereignty itself. Second, states used the word "sovereignty" in reference to other policy documents not necessarily related to cybersecurity. Third, states referred to cyberattacks or other malicious cyber-activities constituting threats to their sovereignty. Finally, states argued that a secure cyberspace would protect their sovereignty. States sometimes used the concept of sovereignty in other contexts that were not relevant for this Trend Analysis. It is worth mentioning that Finland, in its background document to its 2013 Cyber Security Strategy, mentions that it is aware of international discussions regarding whether cyberattacks constitute a use of force or not. Again, France stood out through its use of the concept of sovereignty, which sometimes aligned, but mostly differed from the use of the term by other states.

These findings confirm a lack of shared understanding and definition of the word "sovereignty" in the context of cybersecurity, although states tend to apply the traditional Westphalian definition in their strategies by expressing concerns about cyberattacks and insecure cyberspace constituting threats to their sovereignty.

Year of publication

In terms of the year of publication of national cybersecurity strategies, 55 out of the 93 studied documents were published before and 38 after Edward Snowden's 2013 revelations. Out of 18 documents containing the words "sovereignty" and "cyber sovereignty", 13 documents were published before 2013 and five documents after. However, there is no clear difference in the use of the concept of sovereignty between documents written before 2013 and the ones written later. The only difference lies in the fact that strategies published after 2013 tend to argue more strongly for the necessity of a secure cyberspace in order to ensure state sovereignty.

These results do not confirm the hypothesis that Edward Snowden's revelations caused indignation among states and a resurgence of sovereignty terminology. However, only a minority of documents containing the word "sovereignty" were written after 2013. It is possible that strategies intended for publication in subsequent years may include more references to the protection of state sovereignty in cyberspace.

Review of strategies

As far as updated strategies are concerned, eight states revised their national cybersecurity strategies at least once between 2000 and December 2017. Four of these did not reuse the concept of sovereignty in their new strategies, three used it again and one added the term.

These findings do not confirm any significant change in the use of the concept of sovereignty over time.

3.3 Conclusion

These results demonstrate that, in general, states only use the term "sovereignty" infrequently in their national cybersecurity strategies, and even where they do use the term, they tend to do so rarely and without defining it clearly. Also, states tend not to share a common understanding of the term. However, it appears that the Westphalian understanding of the sovereignty concept prevails among states in the context of cybersecurity. It also appears that, where the concept of sovereignty is used in strategies, its use does not evolve over time and was barely impacted by Edward Snowden's revelations.

The unique case of Canada's 2010 national cybersecurity strategy – the sole document to mention the term "cyber sovereignty" – does not reveal much on the use of the term. It only confirms a certain vagueness maintained around the concept, as it is not clearly defined in the document, which simply states that cyber sovereignty is an important element of Canada's cybersecurity strategy.

While states rarely use the term "sovereignty" in their policy documents, it is possible that they refer to this concept in greater detail in doctrinal documents that may not be publicly available. Sovereignty may also be discussed more informally in domestic and/or international forums, but these discussions are not necessarily made explicit in policies.

Nevertheless, France stands out in any of these observations because of its unique understanding and use of the concept of sovereignty and its express reference to sovereignty in its national cybersecurity strategy. It is possible that other states have a similar approach to sovereignty but are less transparent about it than France.

3.4 Exception: France

In this research, France was unique among the states examined in that it used the word "sovereignty" more frequently and in different contexts. This sub-section examines France's legal definition of sovereignty to establish whether this difference is due to historical, legal or political reasons.

The French constitution from 1958 does not define international sovereignty, only national sovereignty (Combacau, 2001). National sovereignty consists in being the holder of the supreme national authority. This power belongs to the people, who are represented by a political body. This concept was originally introduced during the time of the French Revolution in Article 3 of the 1789 Declaration of the Rights of Man and of the Citizen, which gave sovereignty to the population and its political representatives (Direction de l'information légale et administrative, 2014). This concept of sovereignty is also referred to as popular sovereignty. French popular sovereignty differs from the Westphalian concept of sovereignty in that it is based on a bottom-up rather than a top-down approach. In France, the definition of international sovereignty is based on principles of national sovereignty.

That being said, France's use of the word "sovereignty" in its 2011 national cybersecurity strategies mostly related to potential threats that cyberattacks might pose to its sovereignty (Agence Nationale de la Sécurité des Systèmes d'Informations, 2011). This approach does not differ much from other states' understanding of sovereignty in their national cybersecurity strategies.

However, France's 2015 national digital security strategy places greater emphasis on the need for states to maintain their autonomy in cyberspace through the development of trustworthy technologies and partnerships. There is also an acceptance that states cannot survive without using digital technologies and that these technologies can impact indirectly on state sovereignty (e.g. via the economy or national currency). There are distinct concerns regarding the dominance of certain private companies (e.g. Google, Amazon, Facebook, Apple, and Microsoft) over digital technologies and cyberspace. These concerns relate mostly to the risk that these companies may abuse their power, deploy their technologies against French interests or deny access to cyberspace to French authorities and citizens. The suggested solution to these concerns entails the development of domestic and European industries to counter the monopolistic position of the aforementioned private companies. France's strategy also refers to the sovereignty of other states needing to be respected in cases where France wishes to promote European regulations to increase the European Union's (EU) digital autonomy (Secrétariat Général de la Défense et de la Sécurité Nationale, 2015a).

It is worth mentioning that there are differences between the French version and the English version of the 2015 document. In the French version, the word "sovereignty" (souverainité) is sometimes rendered as "digital strategic autonomy" in English (Secrétariat Général de la Défense et de la Sécurité Nationale, 2015a, 2015b). This substitution, which is mostly found in the part of the strategy that relates to the development of EU autonomy in digital technologies, distinctly confirms that the French understanding of sovereignty is mainly based on the autonomy of actions and decisions. This definition clearly differs from the aforementioned definition based on International Law and leans toward the understanding of the concept from a strategic autonomy perspective.

France is therefore an exception as far as reference to cyber sovereignty in the country's national cybersecurity strategy is concerned. This idiosyncratic approach can be explained in historical terms, as the concept of popular sovereignty and French strategic culture were shaped by the French Revolution. The French understanding of sovereignty in terms of strategic autonomy is derived from French strategic culture, which seeks to achieve this type of autonomy and frames the country as a driving force of the development of strategic autonomy at the level of the EU.

4 Academic debate

The empirical observations showed that most states do not discuss issues of cyber sovereignty in their national cybersecurity strategies. Furthermore, when the internet was developed, its creators wanted it to be immune to state sovereignty. However, academia holds an interesting body of literature on sovereignty in cyberspace. This section will look into this literature and its main debates regarding cyber sovereignty. This investigation provides a better understanding of the main academic discussions in this field and the definition of cyber sovereignty used in academic literature.

4.1 Sovereignty in the context of war

The main theme of academic literature on sovereignty in the context of cybersecurity concerns International Law and more specifically war and its legal rights and obligations.

Applicability of International Law to cyberspace

The overarching debate in academia concerns the applicability of International Law in cyberspace. Cyberspace is a man-made domain that would not exist without human intervention. It transcends boundaries and constitutes a challenge for International Law and states because of its lack of territoriality. On the one hand, cyberspace is dependent on physical infrastructures which fall under territoriality principles. On the other hand, cyber-activities cannot be contained domestically or bound to a territory because of the interconnectedness of cyberspace (Jensen, 2015; Kanuck, 2010). The challenge resides in this immateriality and interconnectedness.

As mentioned above, the UNGGE reaffirmed in 2015 that states should respect and apply the principles of International Law in cyberspace. As a consequence of this decision, cyber-activities are subject to the rights and obligations of International Law (e.g. respecting UN Security Council resolutions and the Law of Armed Conflict) (Jensen, 2015).

In 2013, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) published a non-binding manual on the applicability of International Law to cyber warfare, which was updated in 2017. These so-called Tallinn Manuals explain the current legal debate about the applicability of International Law in the cyber domain in the context of war, specifying, for example, that states are under an obligation to prevent third-party actors from using their information and communication infrastructures to harm another state (Lotrionte, 2013). However, the first Tallinn Manual was criticized because it was prepared upon the request of the NATO CCDCOE and therefore conveyed a largely Western vision of the applicability of International Law in cyberspace, which may not reflect other states' views on the subject. The Tallinn Manual 2.0 tried to correct this weakness by expanding its pool of experts to include more non-NATO members.

Sovereignty and equality in cyberspace

Cyberspace challenges not only the principles of International Law, but also the principle of state sovereignty, and relevant academic discussions revolve around the existence and recognition of state sovereignty in cyberspace. Scholars agree that state sovereignty exists in cyberspace due to the existence of physical infrastructures necessary for the existence of cyberspace, and sovereignty in cyberspace is therefore perceived as an extension of the territorial principle of sovereignty (Franzese, 2009; Lotrionte, 2013).

In International Law, state sovereignty defines rights and obligations. The latter consist of states recognizing other states as sovereign, refraining from intervening in other states' affairs and needing to control actions of actors within their own territories. These elements are applicable in cyberspace according to Jensen (2015), who argued that the recognition of other states' sovereignty in cyberspace consists of states recognizing that other states are sovereign and free to develop their own cyber capabilities without foreign interference. Recognition of states' sovereignty in cyberspace also relates to the principle of equality and implies that states need to regard each other as equals. If the principle of equality is respected, states should also recognize other states as sovereign (Franzese, 2009; Jensen, 2015).

Can a cyberattack constitute use of force?

Another aspect of International Law that has been the subject of academic discussions concerns the definition of the use of force in cyberspace and its possible consequences. This particular issue is concerned with how cyberattacks can qualify as use of force and therefore be considered to constitute a violation of another state's sovereignty. Qualifying a cyberattack as a use of force or act of aggression could trigger the victim state's right of self-defense, which is regarded as a legitimate reason for going to war (Lotrionte, 2013; Stahl, 2011).

It has been suggested that, in practice, states could see cyberattacks as acts of war. Academics appear to agree that a cyberattack on critical national infrastructure that causes damage and can be attributed to a state constitutes a violation of the Law of Armed

Conflict (Lotriionte, 2013). Stuxnet[4], a piece of malware[5] used to damage facilities enriching uranium for nuclear purposes in Iran, is a good example of a cybertool specially designed to cause damage without crossing the threshold of what constitutes an act or war (Rosenbaum, 2012).

The question of responsibility and attribution in cyberspace

However, academic literature continues to identify the attribution part of a cyberattack as a serious challenge. The attribution problem is defined as the uncertainty associated with trying to attribute a cyberattack. Attribution is both a technical activity that is based on technical and circumstantial evidence, and a political act, where state representatives officially and publicly attribute an attack. Cyberattacks cannot be attributed to the actual perpetrator with 100% certainty. There is therefore always the possibility that the accused party may not in fact be the actual attacker. It has been observed that, due to this attribution uncertainty and additional technicalities such as the random routing of data packets, states seem reluctant to accept responsibility for cyber-activities originating from their territories (Jensen, 2015). The question of responsibility is relevant to the academic debate because another state's responsibility is a necessary prerequisite for a state to be able to invoke the right of self-defense. The difficulties tied to the attribution problem and the fact that data randomly jump from one router to another make it easier for states to avoid responsibility. At the same time, states are concerned about being held responsible for malicious cyber-activities transiting their infrastructures.

This issue is further complicated by the problem of non-state actors committing malicious cyber-activities. These actors bring even greater uncertainty to the attribution process, as states may employ, finance or train such actors to attack another state (Lotriionte, 2013; Stahl, 2011). The question of non-state actors perpetrating malicious acts against another state is already a complex issue in International Law outside of cyberspace, as it raises problems regarding state responsibility for controlling or assisting non-state actors. In cyberspace, the problem is even more complicated, as both non-state actors and states are able to play on the attribution problem to avoid responsibility. Another issue in cyberspace is how victim states can respond to non-state actors located within another state's territory. This problem is tied to the question of state responsibility and state control over non-state actors (Lotriionte, 2013).

4.2 Sovereignty in the context of domestic control

Scholars do not solely examine sovereignty in cyberspace in the context of war. There is also the issue of states claiming greater sovereignty over cyberspace by restricting access to internet content within their territories. Some states, among them China, have decided that certain internet content may harm their people and that they need to take action to suppress such content (Lotriionte, 2013). While this is an expression of state sovereignty over its own territory, it also has a political impact on international relations. Demchak and Dombrowski (2013) argue that this type of conduct is evidence of a "Westphalian system" developing in cyberspace.

4.3 Conclusion

Academic debate in this field largely focuses on whether and how International law can and should be applied in cyberspace. It is generally accepted that International Law is applicable in cyberspace, but a number of details, including the definition of the use of force and the attribution problem, still remain to be solved.

[4] For more information on Stuxnet, see Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich.

[5] Technical terms are explained in a glossary in Section 8.

5 Comparison to other domains

This section examines previous discussions of sovereignty in other domains and compares them with the current discussions of sovereignty in cyberspace in order to shed light on how state sovereignty has been applied to these domains. This in turn will further our understanding of the current discussions regarding cyberspace.

5.1 No new debate

The debate revolving around the issue of the applicability of state sovereignty in cyberspace also took place regarding other domains such as sea, air and space. In all of these domains, technology acted as a critical element in states' control over the new domains by creating new economic and military opportunities. However, since states are not equal in their ability to control domains, these new domains needed to be subjected to international regulation. These developments demonstrate that the current discussions regarding the applicability of state sovereignty and associated rights and obligations in cyberspace do not constitute a new debate.

Sovereignty in the maritime domain

The seas were traditionally regarded as a global commons, meaning that they cannot be owned but are available to all. Seas and their resources were open to all, without any state claiming ownership, as early as in Ancient Roman times, with the debate over seas constituting a global commons or belonging to states only starting at the end of the 16th century, as maritime and navigation technologies evolved. By the end of the 17th century, a distinction was made between high seas, which remained open to all, and coastal waters, which states could lay claims to. In the 19th century, these principles came to be seen as falling under International Law, but the extent of coastal waters remained to be defined. The issue was debated between supporters of more extensive coastal waters, who often claimed sovereignty over natural resources such as oil or natural gas, and supporters of more limited coastal waters. The debate was largely resolved by the 1982 UN Convention on the Law of the Sea, which set the limit of territorial waters to twelve nautical miles (United Nations, 1982). States are able to claim sovereignty over waters within this distance from their coasts, although some waters are still contested (Franzese, 2009; Stang, 2013).

Sovereignty in the air domain

Like the seas, air was traditionally regarded as a global commons, although it was generally accepted in Western states that an owner of land also owned the air above it. The concept of air sovereignty only evolved together with the development of aviation. In the early 1900s, a relevant debate emerged between the supporters of free airspace and the supporters of air sovereignty. The latter prevailed in practice, resulting in International Law principles of sovereignty being applied *de facto* to airspace. Air sovereignty became customary international law by the end of the First World War, and the first multilateral agreement to regulate airspace was signed in 1919. The concept of air sovereignty was highlighted by the Convention of Chicago on International Civil Aviation in 1944, which, in its first article, notes that states recognize that all states have sovereignty over the air above their territories (International Civil Aviation Organization, 2006). This Convention formalized the application of International Law principles to sovereignty in airspace. (Franzese, 2009; Kalpokiené and Kalpokas, 2012).

Sovereignty in the space domain

The development of rocket and satellite technology raised the issue of state sovereignty in outer space. Similar to the discussions in the other domains, relevant debate initially focused on the extension of state sovereignty on the basis that air sovereignty was not limited in height. However, because the planet rotates, this would have meant that sovereignty in outer space would need to be shared among states in keeping with the Earth's rotation. It was then decided that this approach to sovereignty would not work in outer space. It was agreed that outer space was a global commons and therefore could not be claimed by any state. This status was formalized in the 1967 Outer Space Treaty, which declares that sovereign states cannot claim outer space or celestial bodies. However, the treaty made it clear that states can be held responsible for their actions in space (Franzese, 2009; Kalpokiené and Kalpokas, 2012; Stang, 2013; United Nations Office for Outer Space Affairs, 1967).

5.2 Comparison with cyberspace

Is cyberspace a global commons?

As previously seen, these three domains are considered to be global commons. As such, they fall under a specific international law regime to regulate their use and possible sovereignty claims. Unfortunately, it is more difficult to determine whether cyberspace should have the status of a global commons or not.

There are various definitions of global commons. The most widely used one comes from economics and describes a global commons as a rivalrous and non-excludable good. Rivalrous means that the consumption

of the good by one consumer reduces the availability of the good to other consumers. Non-excludable means that it is not possible or very difficult to prevent a consumer from consuming the good. As seen previously, global commons are often natural goods such as air and sea. The common ground between all the definitions is that global commons are natural goods in zones that evade the control of individual states and remain accessible to both states and private actors. Currently recognized global commons are the high seas, outer space and Antarctica (Kanuck, 2010; Stang, 2013).

In regard to cyberspace, some argue that it is a global commons because it is rivalrous (a state-user reduces the use of others) and non-excludable (it is difficult to exclude state-users). Also, cyberspace transcends national jurisdictions similar to other domains such as the seas and outer space (Stahl, 2011). Yet others claim that even though cyberspace exhibits some characteristics of global commons, it cannot be considered as such because it is man-made and therefore not a natural resource. They add that most of the physical infrastructures necessary for the functioning of cyberspace are owned by private actors who are subject to national laws, which constitutes another point of difference compared to the other three domains (Franzese, 2009; Kanuck, 2010; Stang, 2013). The discussions on the status of cyberspace as a global commons are still ongoing.

Conclusion

The debate over sovereignty in cyberspace seems to follow a similar pattern as for the other domains. For each domain, there was a period of debate between supporters of sovereignty and supporters of open access, which also included discussions about applicable principles of the use of force and responsibility. At some point, one practice prevailed over the others, and an international law regime was established to formalize the practice under International Law.

The case of cyberspace is still in its early stages, and debates over sovereignty are still ongoing. However, the 2013 UNGGE decision to apply sovereignty principles in cyberspace most likely marked a turn in the process. This decision may eventually lead to a more binding international treaty that will formalize practices in cyberspace. The Tallinn Manual provides good indications of how International Law can be applied in cyberspace, but its contested nature would be a disadvantage if the Manual were to form the basis for a treaty. Nevertheless, cyberspace remains a special case compared to the other domains because of its still undefined status of a global commons.

6 Conclusion

This research has shown that sovereignty in cyberspace revolves around the applicability of International Law in cyberspace. It demonstrates that states have not used the terms "sovereignty" or "cyber sovereignty" frequently in their national cybersecurity policies, but that France follows a different approach. This research further shows that the academic debate on sovereignty in relation to cyberspace has focused on the conditions for applying International Law principles in cyberspace. It also looks into the sovereignty claims that some states have raised in order to control internet contents. Finally, this Trend Analysis shows that similar discussions regarding sovereignty have also occurred in other domains and that cyberspace is currently undergoing a similar process.

However, there is an alternative debate developing in parallel to the academic debate. This discussion mostly originates from the economic sector, but also resonates in the defense sector: There are studies financed by industrial associations in Germany and French public institutions claiming that states should reclaim cyber sovereignty or digital sovereignty. They cite the loss of trust in the US Information Technology (IT) industries following Edward Snowden's revelations as one reason among others for reclaiming cyber or digital sovereignty, which they understand as states having control over the trustworthiness, integrity, availability, transmission, storage and processing of data and over IT infrastructures. In short, they want digital autonomy or a European digital autonomy in the form of a guarantee that third parties will not be able to alter data or infrastructures. They seek to develop domestic IT industries, solutions and expertise to avoid dependence on foreign private actors and/or other states. However, economic actors are clear on the fact that they do not seek self-sufficiency or autarky in the IT sector, and they insist that the best solution would be the development of trustworthy partnerships (Barchnicki et al., 2015; BITKOM, 2015; Borchers, 2015; Poupard, 2016; Techconsult and Lancom Systems, 2015). This alternative debate agrees with the French approach to cyber sovereignty, discussed in Section 3.4. The 2016 EU Data Protection Directive and the 2016 Chinese cybersecurity policy constitute good examples of the emergence of this alternative debate and the fight over the control of data. They both seek to retain data within their respective territories to avoid losing control over it (de Combles de Nayves and Guillot, 2016; Lewis, 2017; Maxey, 2017b, 2017a).

These claims are problematic for several reasons. First, if sovereignty needs to be reclaimed, it means that it has already been lost. However, cyberspace was initially developed to be immune to state sovereignty, and states were therefore not involved in its development and technical governance (Franzese, 2009). States consequently did not have sovereignty in cyberspace in the first place and therefore cannot reclaim it. Second, the trustworthiness and control over data and IT infrastructures do not fall under the principles of state sovereignty, but of strategic autonomy. The latter is important and relevant to asserting state sovereignty but does not constitute sovereignty as such. Third, economic actors demanding more cyber or digital sovereignty are not selfless actors. They hope that a greater focus on domestic IT solutions will increase government spending on national cybersecurity and may deliver political measures (e.g. subsidies, protectionism, contracts) in their favor.

This alternative debate is indicative of a growing misunderstanding of what sovereignty in general, and sovereignty in cyberspace specifically, is. This misunderstanding needs to be rectified. Economic and defense actors wishing for greater control over IT should rather talk about cyber or digital strategic autonomy issues than about cyber or digital sovereignty, as this would help reduce confusion surrounding the term "cyber sovereignty".

7 Annex 1

List of states' cybersecurity and/or cyberdefense strategies used in the words search in section 3.

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
1	Afghanistan	National Cyber Security Strategy of Afghanistan	2014	No	No	-
2	Australia	Cyber Security Strategy	2009	Yes	No	1
3	Australia	Australia's Cyber Security Strategy	2016	No	No	-
4	Austria	National ICT Security Strategy Austria	2012	No	No	-
5	Austria	Austrian Cyber Security Strategy	2013	No	No	-
6	Bangladesh	National Cybersecurity Strategy	2014	No	No	-
7	Belgium	Cyber Security Strategy. Securing Cyberspace	2012	No	No	-
8	Belgium	Defence Cyber Security Strategy	2014	No	No	-
9	Canada	Canada's Cyber Security Strategy	2010	Yes	Yes	2
10	Canada	Action Plan 2010-2015 for Canada's Cyber Security Strategy	2013	Yes	No	1
11	Chile	National Cybersecurity Policy	2017	Yes	No	1
12	China	National Cyberspace Security Strategy	2016	No	No	-
13	Colombia	National Cybersecurity and Cyberdefense Policy	2011	Yes	No	2

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
14	Croatia	The National Cyber Security Strategy of the Republic of Croatia	2015	No	No	-
15	Cyprus	Cybersecurity Strategy of the Republic of Cyprus	2012	No	No	-
16	Czech Republic	National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020	2015	No	No	-
17	Denmark	Danish Cyber and Information Security Strategy	2015	No	No	-
18	Denmark	A stronger and more secure digital Denmark	2016	No	No	-
19	Egypt	National ICT Strategy 2012-2017	2012	No	No	-
20	Estonia	Cyber Security Strategy 2014-2017	2014	No	No	-
21	Finland	Security Strategy for Society	2010	Yes	No	4
22	Finland	Finland's Cyber Security Strategy Background Dossier	2013	Yes	No	2
23	Finland	Finland's Cyber security Strategy	2013	No	No	-
24	France	Information Systems Defence and Security - France's Strategy	2011	Yes	No	9
25	France	French National Digital Security Strategy	2015	Yes	No	5
26	Georgia	Cyber Security Strategy of Georgia 2012-2015	2012	No	No	-

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
27	Germany	Cyber Security Strategy for Germany	2011	Yes	No	1
28	Ghana	Ghana National Cyber Security Policy and Strategy	2014	Yes	No	1
29	Greece	National Cyber Security Strategy	2017	No	No	-
30	Hungary	National Cyber Security Strategy of Hungary	2013	Yes	No	2
31	Iceland	Icelandic National Cyber Security Strategy 2015–2026	2015	No	No	-
32	India	National Cyber Security Policy 2013	2013	No	No	-
33	Ireland	National Cyber Security strategy 2015-2017	2015	No	No	-
34	Israel	Advancing National Cyberspace Capabilities	2011	No	No	-
35	Italy	National Strategic framework For Cyberspace Security	2013	No	No	-
36	Jamaica	National Cyber Security Strategy	2015	No	No	-
37	Japan	Cybersecurity Strategy - Toward a World-Leading, Resilient and Vigorous Cyberspace	2013	Yes	No	1
38	Japan	International Strategy on Cybersecurity Cooperation	2013	No	No	-
39	Japan	Cybersecurity strategy	2015	No	No	-

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
40	Jordan	National Information Assurance and Cyber Security Strategy	2012	No	No	-
41	Kenya	Cybersecurity Strategy	2014	No	No	-
42	Latvia	Cyber Security Strategy of Latvia 2014-2018	2014	No	No	-
43	Lithuania	Programme for the development of electronic information security (cyber-security) for 2011-2019	2011	No	No	-
44	Luxembourg	National Cybersecurity Strategy II	2015	No	No	-
45	Malawi	National ICT Policy	2013	No	No	-
46	Malaysia	National Cyber Security	2006	No	No	-
47	Malta	Malta Cyber Security Strategy 2016	2016	No	No	-
48	Mauritius	National Cyber Security Strategy 2014-2019	2014	No	No	-
49	Micronesia	The Federated States of Micronesia National ICT and Telecommunications Policy	2012	No	No	-
50	Moldova	National Strategy for information society development "Digital Moldova 2020"	2013	No	No	-
51	Montenegro	National Cyber Security Strategy for Montenegro 2013-2017	2013	No	No	-

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
52	Morocco	National Strategy for Information Society and Digital Economy ("Digital Morocco 2013")	2013	No	No	-
53	Netherlands	The Defence Cyber Strategy	2012	No	No	-
54	Netherlands	National Cyber Security Strategy 2	2013	No	No	-
55	New Zealand	New Zealand's Cyber Security Strategy	2011	No	No	-
56	New Zealand	New Zealand's Cyber Security Strategy	2015	No	No	-
57	Nigeria	National cybersecurity Policy	2014	Yes	No	3
58	Norway	Cyber Security Strategy for Norway	2012	No	No	-
59	Philippines	Philippine National Cyber Security Plan 2005	2005	No	No	-
60	Poland	Governmental Program for Protection of Cyberspace for the years 2011-2016	2013	No	No	-
61	Portugal	National Cyber Security Strategy	2015	Yes	No	4
62	Qatar	Qatar National Cyber Security Strategy	2014	No	No	-
63	Republic of Korea	National Cyber Security Masterplan	2011	No	No	-
64	Russia	Information Security Doctrine of the Russian Federation	2000	Yes	No	2

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
65	Russia	Basic Principles for State Policy of the Russian Federation in the Field of International Information Security	2013	No	No	-
66	Rwanda	Rwanda National ICT Strategy and Plan	2011	No	No	-
67	Rwanda	Rwanda ICT Strategic and Action Plan	2015	No	No	-
68	Saint Vincent and the Grenadines	National Information and Communication Technology Strategy and Action Plan	2010	No	No	-
69	Samoa	Samoa National Cybersecurity Strategy 2016-2021	2016	No	No	-
70	Saudi Arabia	National Information Security Strategy in Saudi Arabia	2013	Yes	No	1
71	Singapore	National Cyber Security Masterplan 2018	2013	No	No	-
72	Singapore	Singapore's Cybersecurity Strategy	2016	No	No	-
73	Slovakia	National Strategy for Information Security in the Slovak Republic	2008	No	No	-
74	Slovakia	Cyber Security Concept of the Slovak Republic for 2015-2020	2015	No	No	-
75	Slovenia	Cyber Security Strategy	2016	No	No	-
76	South Africa	National Cybersecurity Policy Framework for South Africa	2015	No	No	-

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
77	Spain	National Cyber Security, a Commitment for Everybody	2012	Yes	No	1
78	Spain	National Cyber Security Strategy	2013	No	No	-
79	Switzerland	National strategy for Switzerland's protection against cyber risks	2012	No	No	-
80	Trinidad and Tobago	National Cyber Security Strategy	2012	No	No	-
81	Turkey	National Cyber Security Strategy and 2013-2014 Action Plan	2013	No	No	-
82	Turkey	2016-2019 National Cyber Security Strategy	2016	No	No	-
83	Uganda	National Information Security Strategy	2011	No	No	-
84	Uganda	National Information Security Policy	2014	No	No	-
85	United Arab Emirates	Dubai Cyber Security Strategy	2017	No	No	-
86	United Kingdom	Cyber Security Strategy of the United Kingdom	2011	No	No	-
87	United Kingdom	National Cyber Security Strategy 2016-2021	2016	Yes	No	1
88	United States of America	The National Strategy to Secure Cyberspace	2003	No	No	-
89	United States of America	Cyberspace Policy Review	2009	No	No	-

#	Country	Strategy title	Year of publication	Mentions "sovereignty"	Mentions "cyber sovereignty"	Number of times the word "sovereignty" is mentioned
90	United States of America	International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World	2011	No	No	-
91	United States of America	Department of Defense Strategy for Operating in Cyberspace	2011	No	No	-
92	United States of America	The DOD Cyber Strategy	2015	No	No	-
93	Vanuatu	National Cybersecurity Policy	2013	No	No	-

8 Glossary

Attribution problem: Difficulty to determine with certainty the perpetrator of a cyberattack. Attackers are more difficult to identify because of their ability to cover tracks, perform spoof cyberattacks, or falsely flag other actors as perpetrators (Hay Newman, 2016).

Data packet: Data is broken down into packets for transmission along certain paths in cyberspace (Techopedia, 2018a).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Routing: Establishment of routes for data packets in cyberspace (Techopedia, 2018b).

9 Abbreviations

CCDCOE	Cooperative Cyber Defence Centre of Excellence
EU	European Union
IT	Information Technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NSA	National Security Agency (USA)
UN	United Nations
UNGGE	United Nations Governmental Group of Experts

10 Bibliography

Agence Nationale de la Sécurité des Systèmes d'Informations, 2011. Information systems defence and security France's strategy.

Barchnicki, S., Barth, M., Carstens, J., Glatz, S., Heyde, S., Klasen, W., Linke, L., Moritz, W.-R., Mühlbauer, H., Pösken, H., Weber, G., 2015. Digitale Souveränität.

BITKOM, 2015. Digitale Souveränität.

Borchers, D., 2015. Cybersicherheitskonferenz: Souveränität ist eine Frage der Definition [WWW Document]. Heise Online. URL https://www.heise.de/newsticker/meldung/Cybersicherheitskonferenz-Souveraenitaet-ist-eine-Frage-der-Definition-2690120.html (accessed 27.10.17).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Combacau, J., 2001. La souveraineté internationale de l'État dans la jurisprudence du Conseil constitutionnel français [WWW Document]. Cons. Const. URL http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/nouveaux-cahiers-du-conseil/cahier-n-9/la-souverainete-internationale-de-l-etat-dans-la-jurisprudence-du-conseil-constitutionnel-francais.52497.html (accessed 04.01.18).

Daillier, P., Forteau, M., Pellet, A., Nguyen Quoc, D., 2009. Droit international public: formation du droit, sujets, relations diplomatiques et consulaires, responsabilité, règlement des différends, maintien de la paix, espaces internationaux, relations économiques, environnement, 8e édition. ed. L.G.D.J., Lextenso éditions, Paris.

de Combles de Nayves, D., Guillot, P., 2016. France, in: The Privacy, Data Protection and Cybersecurity Law Review. Alan Charles Raul, pp. 100–112.

Demchak, C., Dombrowski, P., 2013. Cyber Westphalia: Asserting State Prerogative in Cyberspace. Georget. J. Int. Aff. International Engagement on Cyber III, 29–38.

Digital Watch Observatory, 2017. UN GGE [WWW Document]. Digit. Watch Obs. URL https://dig.watch/processes/ungge (accessed 05.02.18).

Direction de l'information légale et administrative, 2014. La Souveraineté Nationale [WWW Document]. Vie Publique. URL http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/s

ouverainete-nationale.html (accessed 04.01.18).
Franzese, P.W., 2009. Sovereignty in Cyberspace: Can it exist? Air Force Law Rev. 64, 1–42.
Hay Newman, L., 2016. Hacker Lexicon: What is the Attribution Problem? [WWW Document]. WIRED. URL https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/ (accessed 12.01.18).
International Civil Aviation Organization, 2006. Convention on International Civil Aviation.
ITU, 2018. National Strategies Repository [WWW Document]. ITU. URL https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx (accessed 03.01.18).
ITU, 2017. Global Cybersecurity Index 2017 78.
Jensen, E.T., 2015. Cyber Sovereignty: The Way Ahead. Tex. Int. Law J. 50, 276–304.
Jensen, E.T., 2011. Sovereignty and Neutrality in Cyber Conflict. Fordham Int. Law J. 35, 815–841.
Kalpokiené, J., Kalpokas, I., 2012. Hostes Humani Generis: Cyberspace, The Sea, And Sovereign Control. Balt. J. Law Polit. 5, 132–163. https://doi.org/10.2478/v10076-012-0014-y
Kanuck, S., 2010. Sovereign Discourse on Cyber Conflict Under International Law. Tex. Law Rev. 88, 1571–1598.
Lewis, J.A., 2017. Piecemeal Measures Regulate Cyberspace [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/article/tech/cyberspace-defies-international-regulation (accessed 31.10.17).
Lotrionte, C., 2013. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. Emory Int. Law Rev. 26, 825–919.
Maxey, L., 2017. China Officially Ties Internet Restrictions to its own National Security [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/article/tech/china-officially-ties-internet-restrictions-to-its-own-national-security-2 (accessed 31.10.17).
Maxey, L., 2017b. The Worldwide Struggle to Claim Cyber Sovereignty [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/worldwide-struggle-claim-cyber-sovereignty (accessed 26.10.17).
Poupard, G., 2016. Towards European Digital Sovereignty. Eur. Files 36.
Rosenbaum, R., 2012. Richard Clarke on Who Was Behind the Stuxnet Attack [WWW Document]. Smithsonianmag.com. URL http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?no-ist (accessed 19.10.16).
Schmitt, M.N., NATO Cooperative Cyber Defence Centre of Excellence (Eds.), 2017. Tallinn manual 2.0 on the international law applicable to cyber operations, Second edition. ed. Cambridge University Press, Cambridge, United Kingdom ; New York, NY, USA.
Schmitt, M.N., NATO Cooperative Cyber Defence Centre of Excellence (Eds.), 2013. Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press, Cambridge ; New York.
Secrétariat Général de la Défense et de la Sécurité Nationale, 2015a. French National Digital Security Strategy.
Secrétariat Général de la Défense et de la Sécurité Nationale, 2015b. Stratégie Nationale Pour La Sécurité Du Numérique.
Stahl, W.M., 2011. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. Ga. J. Int. Comp. Law 40, 247–273.
Stang, G., 2013. Global Commons: Between Cooperation and Competition.
Techconsult, Lancom Systems, 2015. Digitale Souveränität: Einschätzungen in der deutschen Wirtschaft und Verwaltung.
Techopedia, 2018a. Data Packet [WWW Document]. Techopedia. URL https://www.techopedia.com/definition/6751/data-packet (accessed 16.01.18).
Techopedia, 2018b. Routing [WWW Document]. Techopedia. URL https://www.techopedia.com/definition/13207/routing (accessed 16.01.18).
United Nations, 1982. United Nations Convention on the Law of the Sea.
United Nations General Assembly, 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (No. 15–12404). United Nations.
United Nations Office for Outer Space Affairs, 1967. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.

CSS CYBER DEFENSE PROJECT

Trend Analysis:

Data Sovereignty

Zürich, November 2018

Version 2

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Marie Baezner

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zurich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zurich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching, Andreas Wenger, Director of the CSS

Please cite as: Baezner, Marie (2018). Cyber sovereignty and Data sovereignty, Version 2, Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

1 Definition of data sovereignty

Data sovereignty, like cyber sovereignty, is a vague concept that is often used as a catch-all term. Therefore, for the purpose of this addendum, it is necessary to define precisely what is meant by data sovereignty.

Data sovereignty ultimately relies on the concept of sovereignty itself. As explained in the Trend Analysis on cyber sovereignty, the idea of sovereignty can be traced back to the Peace of Westphalia in 1648. A sovereign state has power and sovereignty over both their physical territories and their domestic affairs. In other words, states have the right to govern themselves as they see fit, and other states must respect that status and resist the urge to interfere (Franzese, 2009). In the modern world, the principle of sovereignty is paramount; it forms the bedrock on which International Law and the international order are built.

Cyber sovereignty in particular has been defined in the Trend Analysis on cyber sovereignty as follows: "the application of principles of state sovereignty to cyberspace" (Baezner and Robin, 2018).

The concern over data sovereignty became increasingly concentrated as cloud computing and internet-based platforms became the standard. Edward Snowden's 2013 revelations about the US internet mass surveillance program only heightened international fears. States were increasingly invested in protecting the data that was created and transiting through their territories. However, data sovereignty is not an established legal concept and therefore understandings can vary greatly (Irion, 2012). Peterson et al (2011) defines data sovereignty as a way to limit the transfer and storage of data to a specific territory. However, this definition lacks the notion of control, and does not include the intention to control data originating from a specific state. De Filippi and McCarthy (2012) describe data sovereignty simply as the possibility for users to have control over their own data but this definition lacks the element of state control over data.

For the purpose of this addendum, the definition of data sovereignty is based on Polatin-Reuben and Wright's (2014) definition: data sovereignty is the states' will to control information generated in or passing through their territory and includes set of measures employed to achieve that control. A critical component of this definition is that states want to attach data to their respective territory, with the intention to protect it from foreign surveillance. It is important to note that Polatin-Reuben and Wright (2014), as well as and Maurer et al. (2015), consider data sovereignty as a subset of cyber sovereignty.

[1] The methodology is explained in details in the main part of the Trend Analysis on Cyber Sovereignty in Section 3.

2 Empirical observations

This section analyzes how, where, and when the term "data sovereignty" is used in national cybersecurity strategies. It uses a similar methodology as the process described in the Trend Analysis on cyber sovereignty.

2.1 Scan of national cybersecurity strategies

In the Trend Analysis on cyber sovereignty, analysis was undertaken by searching for the term "cyber sovereignty" and the word "sovereignty" in national cybersecurity strategies from around the world. A total of 93 publicly available documents written in English were examined.[1] In this addendum, the research analyzed the same documents, as well as new strategies released by Canada and Switzerland in June and April 2018, respectively. As in the Trend Analysis, the research was limited in that it searched for specific words and phrasing, and could not filter for the concepts themselves.

2.2 Results and analysis

While some states mentioned cyber sovereignty and sovereignty in their national cybersecurity strategies, none included the term "data sovereignty." However, this result does not mean that states do not use the term at other political levels or in practice. National cybersecurity strategies reflect a political debate at a particular moment in time. The term may be too recent, too vague, or its aims too ambitious to be included in a national cybersecurity strategy at the moment. States may also use different terminology discuss the same concept. It is also possible that some states have developed classified cloud computing strategies, which may include the term "data sovereignty." There are a number of other doctrinal documents that may employ the term as well, but are not made publicly available. As such, they could not be examined in this addendum.

3 Discussions on data sovereignty

The term "data sovereignty" may not be used in national cybersecurity strategies but the term is nevertheless growing in importance. Discussions about data sovereignty increased after Edward Snowden's revelations on the American mass surveillance program in June 2013. Consequently, states devised several defensive propositions on how data sovereignty might be achieved. This subsection broadly examines some of these technical suggestions, including an analysis of their potential efficiency. Following that, potential legal solutions will be discussed.

3.1 Technical solutions

In their discussions following Snowden's reveal, states prepared several technical solutions to reinforce their data sovereignty. Many of these solutions were directed against US espionage. Germany, alongside several states from Latin America, suggested building an internet submarine cable to bypass the US and connect their two continents directly. They believed that such infrastructure would prevent surveillance and data tampering from the US (Hill, 2014; Maurer et al., 2015; Nugraha et al., 2015). A group of states, including Switzerland and Germany, brought the idea of a Schengen routing network.[2] Data packets would then only transit through internet infrastructure within the defined network. With this solution, tampering or surveillance from any entity outside that network is also hindered (Dönni et al., 2015; Maurer et al., 2015; Nugraha et al., 2015). The European Union (EU)[3] suggested a European cloud service, with servers that could store data located inside the EU. By implementing their own cloud service, the EU would not have to rely on foreign actors to store their data while reducing their exposure to foreign surveillance (Amoore, 2018; Maurer et al., 2015). Germany also suggested its citizens use only German email services that housed their servers in Germany (Hill, 2014; Maurer et al., 2015; Nugraha et al., 2015).

All these ideas have the aim to protect data from surveillance on the internet by rendering access to this data more difficult.

Analysis

Tying data to a specific geographical zone is a popular solution to guard against foreign surveillance, but it can create a false sense of security. Some of the proposed solutions, like building new internet submarine cables or a routing network, would require extensive work. New internet infrastructures and routing protocols would be required, but there would be no guarantee that surveillance could be prevented. Submarine cables can still be tapped and localized routing can still be spied on (Maurer et al., 2015). Other ideas, like a European cloud service or the use of national email services, also do not offer effective prevention against espionage. Storing data on a specific territory can even put data more at risk than if it were spread across the servers of a commercial cloud service. Commercial cloud services tend to move data constantly, looking for increased storage capacity at a lower price point, and to increase the speed and efficiency of the access and retrieval of data (Irion, 2012). Therefore, data stored on multiple servers may be more difficult to intercept than data that always stays in the same infrastructure. Also, perhaps counterintuitively, there are fewer legal restrictions on accessing data stored outside the US. US intelligence agencies need less evidence to get access to a server outside the US than for a server in the US (Hill, 2014). Ultimately, the way data is stored is more important to ensure its security and integrity than its storage location.

3.2 Legal measures

In response to Snowden's revelations and states' growing concerns over data management by cloud computing services, numerous states developed regulations to supervise the use of data stored or collected by third parties. The EU developed the General Data Protection Regulation (GDPR), which came into force in May 2018. This regulation aims to supervise the use of users' data by online third parties. Under the GDPR, third parties require user consent to use their data (Hill, 2014; Mittal et al., 2017). The GDPR also sought to standardize data protection regulations within the EU (Witzleb and Wagner, 2018).

In Brazil, regulatory bodies have considered inscribing data sovereignty as a citizens' right. Snowden's revelations prompted widespread debate over data protection in the Brazilian parliament. Brazil's first internet regulation, the Marco Civil de Internet, was signed in April 2014. The Marco Civil de Internet contains rights for internet users and obligations for internet providers, but it does not contain rules on data storage. In July 2018, the Brazilian parliament signed a bill suggesting the development of a regulation similar to the GDPR (Hill, 2014; Mari, 2018; Nugraha et al., 2015).

China is well known for its tight control over the internet and its opposition to the current state of international internet governance. Chinese authorities passed a Cybersecurity Law at the end of 2016 that took effect in June 2017. The Cybersecurity Law addresses

[2] Technical terms are explained in a glossary in Section 6.

[3] Abbreviations are listed in Section 7.

general cybersecurity issues and is accompanied by more specific regulations called “standards”. One such standard is the ‘Personal Information Security Specification’, which took effect in May 2018. This specification covers the collection, storage, use, sharing, and disclosure of personal data. Chinese authorities used the GDPR as an example to inform their cybersecurity laws, but sought to allow for more flexibility than in the GDPR (Polatin-Reuben and Wright, 2014; Sacks, 2018). The Cybersecurity Law states that foreign companies operating in China are required to give access to their data to the Chinese authorities and store their consumers’ data on servers in China. Chinese authorities justify these measures as ways to fight terrorism and cyberespionage (Maxey, 2017).

Russia, like China, contests current international governance of the internet. Russia has explored primarily legal responses to secure its own data sovereignty. Since July 2014, cloud computing services have been legally obliged to store Russian citizens’ data in Russia (Nugraha et al., 2015; Polatin-Reuben and Wright, 2014).

Brazil, Germany and other states submitted a joint resolution to the United Nations (UN) General Assembly in November 2013. The resolution, considered in part a response to US surveillance, focused on the right to digital privacy and portrayed the issue as an issue of human rights. The UN General Assembly adopted the joint resolution (Hill, 2014; Polatin-Reuben and Wright, 2014).

Analysis

The purpose of regulating the use of data is to limit foreign access and maintain states or consumers’ control over the data that was produced on their territory. Given that many of the regulations are recent, it may be too soon to evaluate their efficiency. Data protection laws is one solution for states who felt betrayed after Snowden’s revelations. New data sovereignty laws have also resulted in an economic boost for domestic Information Technology (IT) businesses. By offering local cloud computing services, businesses could attract their state’s support and even benefit from subsidies earmarked for local IT solutions. With these advantages, local companies may be better positioned to compete with big US IT companies in domestic markets. Yet Hill (2014) argues that legal measures that force companies to store data in the same state as where the data originates would not protect it from foreign surveillance. There are sometimes fewer legal protections against intelligence agencies interfering and accessing data outside their own countries. Also, it would be easier for the state where data is located to have access to domestic data and to surveil it.

Finally, data protection laws cannot fully guard against every data sovereignty issue. Formalized laws only partly prevent foreign surveillance and cannot guarantee a state’s control over data produced in its own territory. The problem is not where the data is located, but rather how it is stored. Laws that instead targeted the minimum security standards for data storage and transfer would be more effective tools to protect data and prevent foreign or domestic surveillance.

4 Conclusion

This addendum has shown that data sovereignty is still a broadly defined concept, and it will be difficult to achieve full data sovereignty in practice. Data sovereignty as it is currently conceptualized falls somewhere between the ideas of cyber sovereignty and digital strategic autonomy.[4] On the one hand, the concept of data sovereignty contains the territorial and jurisdictional elements that are intrinsic to the application of cyber sovereignty. Conversely, data sovereignty closely mirrors the idea of strategic autonomy, as it depends on the will to maintain control over data and to build national IT infrastructures to avoid foreign surveillance.

States have suggested technical and legal solutions to better control the use of data generated on their territory, but no proposed solution currently has the capacity to achieve that aim. Ultimately, all the proposals seem to miss the point that data security does not depend on where data is stored but rather *how* it is stored. Following that, states may be better off investing in education. A British study showed that a majority of the British population does not realize that its activities on social media are used by businesses to generate targeted advertisements and to make profits (Coldicutt, 2018; De Filippi and McCarthy, 2012). Raising awareness among the population about the data it generates and how it is used by companies and/or states could help to improve data sovereignty. As people gain awareness of their own data trail, they may become more cautious about their online activities. However, there may be a generational gap in how online privacy is perceived. The younger generation seems to be less concerned by online privacy issues than the previous generation (De Filippi and McCarthy, 2012). Furthermore, education campaigns would only have an effect on the management of data at the individual level. For managing data at societal levels, for example, other solutions would need to be found.

States could also encourage or promote the use of encryption tools. Encryption would not stop foreign surveillance or data theft, but it would make more difficult and costlier for third parties to access that data. Also, encryption can be applied at different layers of the internet, enabling states to decide if they want to promote encryption at the user or hardware level (Maurer et al., 2015). As populations become increasingly familiar with encryption and its use becomes the standard, the risk of citizen data being access by third parties would be greatly reduced.

Data sovereignty is not only difficult to achieve, but it is also an inherently dangerous concept. Many states that have achieved a degree of data sovereignty are authoritarian regimes. Russia and China tightly control internet content and dissident voices in their cyberspheres. States could use data sovereignty as a justification for repressive measures against their populations.

Since Snowden's revelations in June 2013, state calls for greater data sovereignty seem to have decreased, but the desire for more control still exists. Numerous data protection regulations have been drafted or implemented in the intervening years. Additionally, the nascence of this field means it is still too early to be able to observe the long-term effects of these regulations.

[4] Digital strategic autonomy is a concept that was defined in the Trend Analysis on cyber sovereignty as a national control over information technology infrastructures and the data they produce.

5 Glossary

Data packet: Data is broken down into packets for transmission along certain paths in cyberspace (Techopedia, 2018a).

Routing: Establishment of routes for data packets in cyberspace (Techopedia, 2018b).

6 Abbreviations

EU	European Union
GDPR	General Data Protection Regulation
IT	Information Technology
UN	United Nations

7 Bibliography

Amoore, L., 2018. Cloud geographies: Computing, data, sovereignty. Progress in Human Geography 42, 4–24. https://doi.org/10.1177/0309132516662147

Baezner, M., Robin, P., 2018. Trend Analysis: Cyber Sovereignty.

Coldicutt, R., 2018. Data protection laws are useless if most of us can't locate the information we're agreeing to [WWW Document]. Independent. URL https://www.independent.co.uk/voices/data-protection-gdpr-facebook-cambridge-analytica-legislation-a8320381.html (accessed 13.08.18).

De Filippi, P., McCarthy, S., 2012. Cloud Computing: Centralization and Data Sovereignty. European Journal of law and Technology 3, 1–21.

Dönni, D., Machado, G.S., Tsiaras, C., Stiller, B., 2015. Schengen Routing: A Compliance Analysis, in: Latré, S., Charalambides, M., François, J., Schmitt, C., Stiller, B. (Eds.), Intelligent Mechanisms for Network Configuration and Security. Springer International Publishing, Cham, pp. 100–112. https://doi.org/10.1007/978-3-319-20034-7_11

Franzese, P.W., 2009. Sovereignty in Cyberspace: Can it exist? Air Force Law Review 64, 1–42.

Hill, J.F., 2014. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2430275

Irion, K., 2012. Government Cloud Computing and National Data Sovereignty: Government Cloud Computing and National Data Sovereignty. Policy & Internet 4, 40–71. https://doi.org/10.1002/poi3.10

Mari, A., 2018. Brazil moves forward with online data protection efforts [WWW Document]. ZDNet Europe. URL https://www.zdnet.com/article/brazil-moves-forward-with-online-data-protection-efforts/ (accessed 10.08.18).

Maurer, T., Skierka, I., Morgus, R., Hohmann, 2015. Technological Sovereignty: Missing the Point?, in: 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon 2015): Tallinn, Estonia, 26 - 29 May 2015. IEEE, Piscataway, NJ, pp. 53–68.

Maxey, L., 2017. China Officially Ties Internet Restrictions to its own National Security [WWW Document]. The Cipher Brief. URL https://www.thecipherbrief.com/article/tech/

china-officially-ties-internet-restrictions-to-its-own-national-security-2 (accessed 31.10.17).

Mittal, N., Kumar Sharma, S., Verma, A., Frank, D., 2017. Enterprise data sovereignty: If you love your data, set it free [WWW Document]. Deloitte. URL https://www2.deloitte.com/insights/us/en/focus/tech-trends/2018/data-sovereignty-management.html (accessed 09.07.18).

Nugraha, Y., Kautsarina, Sastrosubroto, A.S., 2015. Towards Data Sovereignty in Cyberspace, in: 2015 3rd International Conference of Information and Communication Technology (ICoICT 2015): Nusa Dua, Bali, Indonesia, 27 - 29 May 2015. IEEE, Piscataway, NJ, pp. 465–471.

Peterson, Z.N.J., Gondree, M., Beverly, R., 2011. A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud, in: Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing. Presented at the HotCloud'11, USENIX Association, Berkeley, CA, USA, p. 5.

Polatin-Reuben, D., Wright, J., 2014. An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. USENIX Association.

Sacks, S., 2018. China's Emerging Data Privacy System and GDPR [WWW Document]. Center for Strategic & International Studies. URL https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr (accessed 09.07.18).

Techopedia, 2018a. Data Packet [WWW Document]. Techopedia. URL https://www.techopedia.com/definition/6751/data-packet (accessed 16.01.18).

Techopedia, 2018b. Routing [WWW Document]. Techopedia. URL https://www.techopedia.com/definition/13207/routing (accessed 16.01.18).

Witzleb, N., Wagner, J., 2018. When is Personal Data "About" or "Relating To" an Individual? A Comparison of Australian, Canadian and EU Data Protection and Privacy Laws. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3189376

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.