ACIG
APPLIED CYBERSECURITY
& INTERNET GOVERNANCE

NASK

The Cybersecurity Obligations of States Perceived as Platforms: Are Current European National Cybersecurity Strategies Enough?

Vagelis Papakonstantinou Faculty of Law and Criminology, Vrije Universiteit Brussel, Belgium, ORCID: 0000-0002-2536-2951

Abstract

Cybersecurity is a relatively recent addition to the list of preoccupations for modern states. The forceful emergence of the internet and computer networks and their subsequent prevalence quickly brought this to the fore. By now, it is inconceivable that modern administrations, whether public or private, can exist entirely outside the digital realm. Nevertheless, with great opportunities also comes great risk. Attacks against computer systems quickly evolved from marginalised incidents to matters of state concern. The exponential increase in the importance of cybersecurity over the past few years has led to a multi-level response. New policies, followed by relevant laws and regulations, have been introduced at national and international levels. While modern states have therefore been compelled to devise concrete cybersecurity strategies in response to potential threats, the most notable aspect of these strategies is their resemblance to one another. Such uniform thinking could develop into a risk per se: challenges may appear unexpectedly, given the dynamic nature of the internet and the multitude of actors and sources of risk, which could put common knowledge, or what may be called conventional wisdom, to the test at a stage where the scope for response is limited. This paper builds upon the idea of national states being perceived as platforms within the contemporary digital and regulatory environment. Platforms are in this context information structures or systems, whereby the primary role of states acting as platforms is that of an information broker for its citizens or subjects. This role takes precedence even over the fundamental obligation of states to provide security; it calls upon them first to co-create (basic) personal data, and then to safely store and further transmit such data. Once the key concept of states as platforms has been

Received: 04.10.2022
Accepted: 29.11.2022
Published: 03.12.2022

Cite this article as:
V. Papakonstantinou, “The Cybersecurity Obligations of States Perceived as Platforms: Are Current European National Cybersecurity Strategies enough?,” ACIG, vol. 1, no. 1, 2022, DOI: 10.5604/01.3001.0016.1237

Corresponding author:
Vagelis Papakonstantinou, Faculty of Law and Criminology, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium,
ORCID: 0000-0002-2536-2951;
E-mail:
vagelis.papakonstantinou@vub.be

elaborated in section 2, this paper then presents the concrete consequences of this approach within the cybersecurity field. In section 3, former off-line practices for safely storing personal information, undertaken by states within their role as platforms, are contrasted with the challenges posed by the digitisation of information. The focus is then turned in section 4 to the EU, and the NIS Directive's obligation upon Member States to introduce and implement national cybersecurity strategies, which are therefore examined under the lens introduced in section 2. Finally, specific points for improvement and relevant recommendations for these cybersecurity strategies are presented in section 5.

Keywords
data localisation, digital sovereignty, national cybersecurity strategies, states as platforms

1. Introduction

Cybersecurity is a relatively recent addition to the list of preoccupations for modern states. The forceful emergence of the internet and computer networks and their subsequent prevalence quickly brought this to the fore. The use of the internet in public and private administrations developed rapidly from a useful accessory into an inherent, embedded element of all relevant policies and strategies. By now, it is inconceivable that modern administrations, whether public or private, can exist entirely outside the digital realm. Nevertheless, with great opportunities also comes great risk. Attacks against computer systems quickly evolved from marginalised incidents to matters of state concern. Cybersecurity, notwithstanding the definition found in the EU's Cybersecurity Act[1], is a broad term encompassing anything from private security on a standalone computer for personal use to state security and cyberwarfare. It is under this latter context that the term will be used in this paper, to refer to the obligation of modern states to provide and prioritise a secure cyber environment for their citizens or subjects, in order to protect them against cyberthreats and cyberattacks.

The exponential increase in the importance of cybersecurity over the past few years has led to a multi-level response. New policies, followed by relevant laws and regulations, have been introduced at national and international level. New academic interest has emerged (as is apparent from the release of this first issue of an aspiring new academic journal), adding to the traditional studies on security. A new market has also emerged, aimed at satisfying increased consumer and business needs in this sphere. Perhaps the most notable aspect of these responses, however, is that modern states have been compelled to devise concrete cybersecurity strategies. The aim of these strategies is twofold, both to protect and to reassure. States need to protect their citizens and assets from cyberattacks and cyberthreats through specific cybersecurity measures[2]. They also need to be able to demonstrate to their citizens that they are aware of the risk and are taking mitigating measures in tandem that respect the political, historical and cultural circumstances of the societies concerned. National cybersecurity strategies, as published on the internet, need to attain both of these targets.

Nevertheless, the commonality of computer network technologies and of the internet itself (including the digital means to cause harm) has led to considerable harmonisation among state responses. In other words, national cybersecurity strategies mandated by EU law (as made available over the internet) more or less resemble one another. Admittedly, harmonisation has been an explicit aim at both the regional (EU) and international level. Either under a formal legal obligation or within a best practice context, modern states have formulated public national cybersecurity strategies that are similar, both in terms of their assumptions and with regard to their aims and purposes (typically also including the means to accomplish them). However, such uniform thinking could develop into a risk *per se*: challenges, in the form of cyber risks, may arise unexpectedly, given the dynamic nature of the internet and the multitude of actors and

[1] "Cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats", Art. 2(1), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[2] For Europe, this obligation is introduced most prominently in the text of the NIS Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union), whereby Member States are obliged to adopt a national strategy on the security of network and information systems (Art. 1 par. 2(a), where the latter is defined as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" in its Art. 2(2).

sources of risk, which could put common knowledge (or received wisdom) to the test at a stage where the scope for response is constrained.

This paper builds upon the idea of national states being perceived as platforms within the contemporary digital and regulatory environment [1]. In this context, it elaborates upon a concrete consequence of states-as-platforms within the cybersecurity field. To this end, section 2 introduces the idea of states as platforms; section 3 then particularizes this general discussion by specifically referring to the cybersecurity field, in an attempt to highlight specific consequences of states being perceived as platforms. The focus is then turned to the EU, and the NIS Directive's obligation upon Member States to introduce and implement national cybersecurity strategies, which are therefore examined under the lens introduced in section 2. Finally, specific points for improvement in these cybersecurity strategies are presented in section 5.

2. States as Platforms

The recent adoption, in July 2022, by the European Parliament of the Digital Services Act[3] means that, once it officially comes into effect, it will formally introduce into EU law the term "online platforms": these (at least according to the Commission's original proposal) are meant to constitute "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information"[4], whereby a hosting service, in turn, "consists of the storage of information provided by, and at the request of, a recipient of the service"[5]. Therefore, between the DSA and the Digital Markets Act[6], which was simultaneously adopted as part of a single "Digital Services Act package", a comprehensive framework for the regulation of online platforms is introduced in EU law, the first of its kind both in Europe and internationally.

What constitutes a platform, the projection of which in the digital environment has recently attracted so much of the EU legislator's attention? The legislative definition seen above focuses on what online platforms do, not on what they are. In essence, online platforms are information structures or systems based on software. It is in this (digitised) context that the term is used in EU law. However, in the real, non-digital world the term literally denotes a "flat raised area or structure" (Cambridge dictionary) or "a raised level surface on which people or things can stand" (Oxford dictionary). In real-world usage the term has been employed metaphorically to denote sets of policies or ideas. What is common in both cases is differentiation, even exceptionalism. The concept of a platform may represent something raised above the mundane, or even a singular grouping of ideas, which differentiates it from all others. But there is also the matter of context – where a platform has interconnectedness with other platforms around it: a platform cannot exist in the void. Finally, platforms are structured around basic rules (whether behavioural, regulatory, or other) that are common to all their supporters or users. It is perhaps these characteristics of real-world platforms that rendered the word apt for describing large information systems in the digital world.

The EU's first attempt to regulate online platforms came through the so-called P2B Regulation (platforms-to-business relations Regulation)[7]. In the Commission's words, the P2B Regulation is the "first ever set of rules for creating a fair, transparent and predictable business environment for smaller businesses and traders on online platforms" [2]. While the P2B Regulation therefore aims at regulating the relationship of online platforms with their business users, it is the DSA, and to a lesser extent the DMA, that are expected to govern the other side of the spectrum, namely the relationships between online platforms and their individual users or consumers.

However, European regulatory innovation in the field perhaps invites a different viewpoint: could states themselves be considered as platforms? What if this newly finalised EU regulatory framework was applied to states also? What insights could be derived into the role of states from EU online platform regulation?

[3] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final (the "DSA").

[4] Art. 2, point (h), DSA.

[5] Art. 2, point (f), DSA.

[6] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final (the "DMA").

[7] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

In order to address these questions, the first step lies in uncovering the basic role of states as information brokers. Although this realisation did not become evident until the Information Revolution gave importance to the role of information in human lives, states – within the meaning of organised societies – are first and foremost information brokers for their subjects or citizens[8]. At the moment of birth humans are vested with state-provided information: a name[9], as well as a specific nationality [6, p. 75]. Without these a person cannot officially exist. A nameless individual is unthinkable in human societies. Although it is the family that provides a person with a name when he or she is born, without a specific mechanism to formally acknowledge it such a name could function only among a very small number of people[10]. It is therefore a state (in the above meaning) that, at first, validates a name for a person and then is responsible for its safekeeping through specific bureaucratic mechanisms (or at least its safekeeping is in the state's best interest). The second type of essential information provided by the state at the time of birth of any individual is nationality, in the sense of belonging to a specific state or organised society. Just as is true for names, a stateless person is unthinkable in human societies.

The above two sets of information are subsequently much more enriched within modern, bureaucratic states. Education and employment, family status, property rights, taxation and social security is all information (co-) created[11] by states and their citizens or subjects. For the purposes of this analysis, this type of personal information shall be designated as "basic personal data". It is after basic personal data have been created that the second, equally crucial, part of the role of states as information brokers comes into play: states safely store and further disseminate personal data. This is of paramount, fundamental importance to individuals. In order to go about their lives in any meaningful manner, it is imperative that individuals first have their basic personal data stored safely, and then for such data to be readily communicable by their respective state as required. As regards storage, individuals need their basic personal data stored securely for the duration of their lives and for a short period thereafter (at least until all their property rights expire). They need this information to be persistent and not to be tampered with, in order for them to be able to enter into any transaction with third parties over the course of their lives. Second, individuals need this information disseminated to third parties through the intermediation of the state granting validity to the transmission. Trust in human transactions is tacitly provided by the state, through its validation (or even direct transmission) of the personal information concerned.

Information brokerage is therefore the primary role of the state, which takes precedence over any other. No political or state organisation theory can provide individuals with any meaningful life, without their basic personal information safely stored and further transmittable. Accordingly, if a state "loses" a birth certificate or a family record, the persons concerned need to immediately replace them with the assistance of another state, otherwise they will be placed in a state of limbo – and thus in great insecurity. Ultimately, what has already been identified in Hobbes' *Leviathan* as the most fundamental role of a state, the provision of security, would be meaningless unless that state's function as an information broker has already occurred, meaning that the state knows who it has to protect[12].

Once the extremely important role of information brokerage for their citizens has been acknowledged, the next step for states is to relate this role with the platforms that have recently captured the EU legislator's attention. Can states in fact be viewed as platforms? Firstly, one could easily remove the digital elements in the EU's definition of online platforms. In essence, the DSA's definition may well apply in the real world too: platforms store and disseminate information to the public at the request of their users. A state viewed as a platform would then form the intermediary in an information flow from its citizens (users, individuals) to everybody else. From this perspective, platforms essentially coincide with the state as information broker, in the manner described above.

[8] Although the role of states assembling "informational capital" has been identified for example by Bourdieu [3, p. 213], this is different than the state's effort to "measure, count, assess, investigate".

[9] Although this is certainly true in modern, centralised bureaucratic states, the same has arguably been the case in any organised society, regardless of whether it was within an iron age empire, a city-state, the Roman empire, Medieval Europe etc. [4]. In other words, ever since the first organised human societies emerged, individuals needed to be registered, if not for anything else then for taxation and military service purposes [5, p. XI].

[10] Although Herzog notes that "for many years historians assumed that there were absolutely no rules indicating who would be called what, or guaranteeing that a person would use the same name throughout his or her life" [7, p. 199], for the purposes of this paper actual use is irrelevant; keeping also in mind the state's best interest in having consistency of names, whether any given person lives an extremely static life and therefore is in no need of a formal name is beside the point.

[11] The role of the state, however, is not that of a trusted third party. The state does not simply safeguard information on its subjects that was created by the subjects themselves but instead actively participates in its creation, by establishing and maintaining the institutions within which creation of this information becomes possible.

[12] Similarly, if under a different political theory the primary role of the state is justice, the state still needs to know who its recipients are.

Or, in other words, states have actually functioned as platforms, albeit in the real world, since the first organised societies emerged.

3. Cybersecurity obligations of States-as-Platforms

The importance of such safekeeping cannot be overstated. As explained in section 2, a nameless or stateless person is out of the question. Similarly, within contemporary societies a person without any family, education or employment data risks living a marginalised and precarious existence. The only entities capable and in charge of safekeeping this information are states. It is their responsibility first to enable the creation and access of this information to individuals (the ownership question over such information notwithstanding), and, once that task has been completed, to make sure that this information remains available and transmittable to any third party at the request of the individuals concerned. States-as-platforms have exclusivity over this extremely important role.

If seen as platforms whose most fundamental role is to store and transmit the basic personal data of citizens to third parties, states carry a specific set of responsibilities. Within the traditional field of security the focus is on individuals themselves [8, 9]: their security, in the sense of physical and psychological well-being, as well as (depending on the theory adopted) their ability to flourish within society, largely dominate the relevant discourse. That same individual's information has attracted much less attention in this regard. However, from a states-as-platforms perspective, the focus turns clearly towards the basic personal data itself: if information brokerage is what states primarily do, and states are the primary providers of a right to security as their most basic *raison d'être,* then such information needs to remain secure, first and foremost.

The security of individuals' basic personal data is therefore crucial. The type of security measures assumed so far by states in order to warrant this inevitably stemmed from the nature of the data stored. Until recently, all basic personal data were registered in paper records, which were kept manually [10]. Digitisation of information came quite late in human history, and much later in public administration[13]. A number of important realisations arise from this understanding. The first is that paper record-creation and record-keeping remained one of the basic functions of state administrations. Once printing became available, paper public records were meticulously created by hand and organised in elaborate filing systems [11]. Their maintenance was of utmost importance: paper records necessary to carry out transactions (i.e. pertaining to living individuals) were carefully kept, updated and preserved. Photocopies and photography assisted this process. Although a relevant analysis of this process goes beyond the scope of this paper, here it is sufficient to note that paper record-keeping has been the norm until very recently, when it comes to states operating as information brokers for their citizens or subjects.

The second realisation refers to the fact that states kept all their basic personal data locally, meaning within their respective territories and jurisdictions. This was unavoidable, given the nature of the data concerned: paper records (or, much less, records kept in stone or any other material) could not be moved from one state to another, either for safekeeping or for any other conceivable reason. This is an important clarification, directly connected to contemporary discussions on digital sovereignty (see the analysis in section 4). Throughout their history (and under whatever political system they maintained) states were never locally separated from the basic personal data of their citizens or subjects. All creation, safekeeping and transmission was performed locally, within their borders; whenever a formal, case-specific transmission to a third state became necessary, elaborate schemes[14] were agreed among states, basically affording cross-platform transmission of information (in essence, platform interoperability).

The third realisation refers to the proportionality of the security measures assumed by states to protect the basic personal data of their citizens. Paper records containing their citizens' basic personal data were kept in state buildings.

[13] The reason behind the GDPR's automated and non-automated files is a legacy provision of its predecessor, the 1994 Directive, which in turn included it because most public sector files in Europe were not digitized until the early nineties.

[14] See, for example, the Hague Treaty (Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents (HCCH 1961 Apostille Convention)).

State buildings are protected both by state authorities (the police) and by the law: in most countries the destruction of public property is a serious crime. Of course, at a higher level, states themselves, including their paper records, are protected by their military forces against attacks from any other state. Consequently, as physical objects of great importance, public records (including the basic personal data) were kept with utmost care by states, raising the level of proportional protection measures to the highest level possible afforded by the state concerned.

Notwithstanding public record-keeping theory and practice, for the purposes of this paper it should be clarified that, as long as basic digital personal data are concerned, the obligations of states as platforms fall within the cybersecurity field. Once digitised, basic personal data lose their tangible nature and existence in the real world and exist only electronically (the same, of course, applying to digital-born data as well). They are no longer paper records, that need to be physically preserved and delivered manually upon request to any party concerned. They are digital records that are transmitted electronically, over the internet or otherwise. In addition, digital state records no longer have a real-world equivalent: electronically created state records containing basic personal data are not additionally printed in paper form, either for safekeeping or for any other purpose. Consequently, if they are deleted for any reason, electronic records are lost forever. While of course this has always been a risk with paper records too, which can be lost or destroyed through natural disasters (e.g. fire or flood) or wilful acts (e.g. war), the risk in such case is admittedly much lower: when it comes to electronic files, pressing a button may lead to the deletion of huge volumes of data in a split second, whereas the burning or flooding of paper records held by the state doesn't occur instantly, and the rate of destruction would most likely be limited due to localisation of the records concerned. The digitalisation of information has allowed state administrations to change their centuries-old methodology of record-creation and safekeeping, moving from a tangible to an intangible format. It is under this change that the states-as-platforms obligations within the cybersecurity context become visible.

A further realisation stems from the digitalisation of basic personal data: other than their increased transferability and, perhaps, vulnerability when compared to their (paper) predecessors, they also enable more efficient state administration. This is a realistic (electronic records are easier to manage than paper records by the same civil servant) and also powerful assumption that has had multiple legal repercussions in the past: namely, it led to the introduction of a new field of law – data protection law – in the 1970s [12, p. 50], and has also led to important case law, such as *Google Spain* and the right to de-listing from online search engines[15]. Consequently, the automation of the processing of basic personal data is of great importance. While in peaceful Western societies this realisation is mostly a benign one, inviting analyses, for example, on how to balance data management optimisation against protection of individual rights, the future ought not be taken for granted: in the event of war, a foreign administration seizing the digitised state records of the defeated state's subjects and citizens will find in its hands a powerful tool of occupation and repression.

The above realisations are by no means intended to constitute an exhaustive analysis of the risks posed to modern states by the digitalisation of state records, particularly those including basic personal data. The aim of the analysis is to highlight the new challenges that states-as-platforms are faced with in the digital realm. While some of these challenges were also present in the past, under the basic role of states as information brokers as seen in section 2, they were largely tacitly mitigated, if not supressed, by the nature of the information *per se:* paper records are neither movable nor easily perishable or easily manageable. Digitised records, however, present none of these faculties: on the contrary, they are easily transmittable, deletable *en masse*, and automatically processable. It is precisely from this perspective that states-as-platforms need to take note, as part of their cybersecurity policies and strategies.

[15] The ruling of the CJEU specifically refers to "processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous", Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, p. 80.

4. Two important shortcomings in European national cybersecurity strategies

The obligation of EU Member States to introduce national cybersecurity strategies ("NCSS") was formally introduced relatively late, in 2016, by the NIS Directive [13, p. 6]. Although cybersecurity risks were acknowledged at the EU level many years ago [14], and in spite of the fact that at the time when the NIS Directive came into effect a number of European countries had already introduced cybersecurity strategies within their respective jurisdictions [15, p. 7, 16, p. 55], horizontal implementation throughout Europe was achieved only through the NIS Directive. In addition to this basic contribution to Member States' cybersecurity, the NIS Directive's other major contribution was the delineation of the contents of such a strategy within its text: according to Article 7 par. 1, such a strategy would have to at least address seven topics, namely: (I) the objectives and priorities of the national strategy on the security of network and information systems, (II) a governance framework to achieve them, (III) the identification of measures relating to preparedness, response and recovery, (IV) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems, (V) an indication of the research and development plans relating to the national strategy on the security of network and information systems, (VI) a risk assessment plan, and (VII) a list of the various actors involved in the implementation of such national strategy. The Commission's approach was later confirmed in the text of the EU Cybersecurity Act[16], as well as in the text of the NIS2 Directive[17]. The new EU's new cybersecurity strategy, released in late 2020, further articulated three areas of EU action, namely (a) resilience, technological sovereignty and leadership, (b) operational capacity to prevent, deter and respond, and (c) cooperation to advance a global and open cyberspace [17, p. 4].

In case they need it, European states are authorised by the NIS2 Directive to ask ENISA, the EU agency for cybersecurity for assistance[18]. On its part ENISA duly obliged, releasing a series of documents to this end, in view of the fact that its involvement in the field had started as early as 2012 [18]: among other things, ENISA has issued a relevant Good Practice Guide [19] and a National Capabilities Assessment Framework [20], together with a guide outlining good practices in innovation on cybersecurity under the NCSS [21]. ENISA also provides an online monitoring tool, the ENISA NCSS Map, conveniently listing all NCSS applicable in the EU, including their strategic objectives and model examples of implementation[19].

Although a detailed comparison of all EU Member States' NCSS lies outside the purposes of this paper, comparative reading immediately makes apparent the impression made upon them both by the European Commission's approach, as included in the NIS2 Directive, as well as by the ENISA guidance. Specifically, in observance to their NIS2 Directive obligations, all Member States have published NCSS, which in greater or lesser detail address the seven points of Article 7 seen above. In addition, all these NCSS have to a large extent taken into consideration ENISA's Good Practice Guide [22, p. 110], as acknowledged in ENISA's National Capabilities Assessment Framework: ".. the disparity between the different Member States makes it difficult to identify common activities or action plans among different national contexts, legal frameworks and political agendas. However, Member States' NCSS's often have strategic objectives articulated around the same topics. Thus, based on ENISA's previous work and the analysis of Member States' NCSS's, 22 strategic objectives were identified" [20, p. 11]. In this manner the NIS Directive seems to have attained a harmonisation effect, in the sense that a few years after its introduction all EU Member States' NCSS appear aligned[20]. Evidently, not all information pertaining to these NCSS is public: because this is ultimately a matter of national security, it is possible that Member States make public through their NCSS[21] only those parts of their actual cybersecurity strategies that are necessary to comply with EU law, not wishing to compromise in this manner any national security state secrets.

[16] See its Art. 2(3).

[17] See Art. 7, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[18] See Art. 7 par. 4 of the NIS2 Directive.

[19] Information from ENISA's website, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

[20] According to Baezner and Cordey, who carried out a comparative NCSS analysis in 2019, cybersecurity strategies shared "a number of common conceptual elements", differences being mostly traced "in where cybersecurity is positioned within the context of government structures, and who bears which responsibilities" [15, p. 4].

[21] And, in fact, translated into English for most countries as early as in 2013 [23, p. 7].

At any event, from a states-as-platforms perspective at least two shortcomings may be identified in current European NCSS implementations: first and foremost, they consider all information to be of equal status. Nevertheless, critical infrastructures notwithstanding, not all information is of equal importance to others. While long debates could be held within a risk assessment analysis over which data relating to critical infrastructure are more important than others, or which digital assets are of higher value, the fact remains that basic personal data ultimately trump all others: if names or nationality information are tampered with or even permanently deleted[22], the effect could be devastating for the individuals and the states concerned. The same would apply to family, education, employment, and tax data. From the point of view of individuals and states, any deletion or tampering with these data would have a devastating effect, whereas any unauthorised access to, for example, bank transactions or the transport system would of course create major problems but scarcely on a similar scale.

The second shortcoming refers to treatment of data security in the event of defeat. Admittedly, the case of loss is addressed through resilience in cybersecurity strategies: the ability of a state to recover in case its protective measures fail [24, p. 29, 25, p. 6]. Defeat is, however, something larger: It means that another state has assumed, through an aggressive act of war, the defeated party's role. What happens then? The reply invites ethical and technical considerations. Should the defeated state accept defeat and assist the winner in assuming its role of managing the lives of its newly acquired subjects, or not? Should state records, particularly including basic personal information, be seamlessly handed over, or not? Depending on the reply to these fundamental questions, different strategies need to be devised. Although addressing these questions would largely be dependent upon political, societal and financial factors, the fact remains that under a states-as-platforms perspective the states concerned need to have made up their mind on these topics and apply specific measures in their national cybersecurity strategies accordingly.

5. Points for improvement

A divergence between the obligations of states-as-platforms and current national cybersecurity strategies is therefore evident from the points made above. As seen in section 3, states viewed as information brokers carry increased responsibilities towards their citizens in view of the digitisation of information. Such increased responsibilities need to be reflected in their respective cybersecurity strategies. EU and Member State national cybersecurity strategies do not appear to fare well under the above criteria: because they are focused more on protective and mitigation measures, they do not take into account the sensitivity of certain categories of information or the event of failure to protect data or even suffer defeat in case of war. It is in this context that certain recommendations will be outlined in this section. This is done not with the intention of compiling a comprehensive list of cybersecurity measures to address the above concerns, but rather by way of presenting examples, in order to attempt a paradigm shift in contemporary cybersecurity national strategies' thinking.

From a cybersecurity perspective, states have to take into account the importance of basic personal information on the one hand, and their role as information brokers on the other hand. The Information Revolution only served to accentuate and bring to the fore their role and responsibility within the states-as-platforms context. Since being a nameless and stateless person is unthinkable in the modern age, states need to ensure that nothing happens to digital records in this regard. Records kept on paper benefited from natural protection, being hard to destroy completely (and even harder to alter) and kept in state buildings, protected by law, the police, and ultimately the military forces of the state concerned. On the contrary, state records that are either digitised or born-digital are easier to destroy or alter and may not even be stored in state-run premises but rather outsourced to the private sector, even outside state borders. Within a states-as-platforms context, all of the above factors need to change: born-digital or

[22] It should be noted that this is a fundamentally different case to identity theft: while identity theft customarily pertains to fraud or other (cyber) crime, in this case state records containing basic personal data may be endangered for national security aims and purposes.

digitised state data, including a person's basic personal data, need to acquire the highest level possible of protection as a digital record, must be kept by the state itself (not outsourced to the private sector), maintained within that state's borders, and ultimately protected physically and electronically by that state's military. It is only in this way that the state will be able to continue serving its fundamental role as an information broker to its citizens. Notwithstanding the adage that "100% security is impossible", the fact remains that states, as is true for records kept in stone or paper throughout human history, have to do everything within their power to keep basic personal data safe.

Once security has been provided, mitigation measures towards worst-case scenarios ought not be overlooked. For example, a successful cyberattack could achieve deletion or alteration of born-digital state records including basic personal data, therefore creating insurmountable difficulties to the state and individuals concerned: mitigation measures need not only be technical and organisational (for example, encryption of the data or their dispersal to several physical locations) but also legal, ultimately leading to proof of identity by real-world means. Similarly, in the event of war won by an aggressor state it must be assumed that all state records of the defeated party will be taken over as well. Because these records include the basic personal data of that defeated state's citizens, they could constitute an extremely powerful tool for oppression, mismanagement, reshaping the previous state's nation-building narrative or discouraging opposition. Individuals subject to digitised or born-digital records will have limited means of resistance available to them, in the sense of providing adequate proof to amend or restore their compromised state records. Mitigation measures within national cybersecurity strategies need to be employed in this regard.

Finally, on a less basic but also important level, states-as-platforms need to carefully and diligently preserve the digital footprint of their citizens as well. While this is of course an already acknowledged task, in most cases it is carried out as part of states' archivist or cultural heritage tasks[23]. However, within the context discussed above, digital preservation is no longer a cultural priority but also a security one. In the event of loss or alteration of state records, the digital lives of their citizens, even if created under an informal, i.e. private capacity, may serve as means of proof or digital evidence. They may serve to contradict affected state records or to cross-reference information in order to prove a claim that, after in the wake of a successful cyberattack, may no longer be tenable. As a result, states operating within a states-as-platforms context need to make the relevant provisions in their national cybersecurity strategies.

6. Conclusions

In 1669 the Venetians, leaving the island of Crete to its new occupiers, the Ottomans, negotiated and successfully managed to take the state archives with them to Italy. In the back of their minds they thought to re-establish themselves on the island in the future (something that they subsequently tried but failed to accomplish), and these records would be crucial in this regard [26, p. 203][24]. State records, particularly when including basic personal data, have long since been invaluable in the event of military conflict. Whether digitised or born-digital, such records set new standards and pose new challenges to this much older discussion.

Even though states have always operated first and foremost as information brokers for their citizens or subjects, it is the Information Revolution that has undeniably brought this role to the fore. Within a states-as-platforms context, states have increased responsibilities and obligations as regards their citizens' personal information, especially when referring to basic personal data. Questions of state survival and continuity, especially when placed alongside human survival and well-being in the case of war (or even defeat), need to be re-visited and re-assessed within the digital environment, where, among other things, digitised or born-digital state records are, by their very nature, easier to destroy, alter or transfer than their older paper counterparts.

[23] For ease of reference simply refer to the UK's National Archives webpage, where it is stated that "We are [...] the official archive and publisher for the UK Government, and for England and Wales. We are the guardians of over 1,000 years of iconic national documents. We are expert advisers in information and records management and are a cultural, academic and heritage institution. We fulfil a leadership role for the archive sector and work to secure the future of physical and digital records", as well as "We collect and secure the future of the government record, from Shakespeare's will to tweets from Downing Street, to preserve it for generations to come".

[24] The same negotiation seems to have occurred hundreds of years later, during the Greek and Turkish population "exchange" in 1924 [27, p. 324].

It is from this, perhaps novel, approach that EU Member States' cybersecurity strategies also need to be assessed. In their current format (as far as openly made public), they suffer from at least two shortcomings when viewed from a states-as-platforms perspective: they treat all information as equal (even when taking into account the critical infrastructure discussion) and they take no account of the case of defeat. While this paper does not purport to compile a comprehensive list of mitigation measures in this regard, it makes the point for data localisation and exclusivity of state protection in order for states to adequately support their role as information platforms for their citizens [28].

REFERENCES

[1] V. Papakonstantinou, "States as platforms following the new EU regulations on online platforms," *European View*, vol. 21, no. 2, pp. 214–222, 2022, doi: 10.1177/17816858221134748.

[2] European Commission. (2019, Feb. 14). *Press Release: Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms' trading practices.* [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168. [Accessed: Sep. 1, 2022].

[3] P. Bourdieu, *On the state: Lectures at the Collège de France, 1989–1992*. Cambridge: Polity, 2015.

[4] K. Breckenridge, S. Szreter, Eds., *Registration and recognition: Documenting the person in world history*. Oxford: Oxford University Press, 2012.

[5] C. A. Bayly, "Foreword," in *Registration and recognition: Documenting the person in world history*, K. Breckenridge, S. Szreter, Eds. Oxford: Oxford University Press, 2012.

[6] G. W. F. Hegel, *Hegel: Elements of the philosophy of right*. Cambridge: Cambridge University Press, 1991.

[7] T. Herzog, "Naming, identifying and authorizing movement in early modern Spain and Spanish America," in *Registration and recognition: Documenting the person in world history*, K. Breckenridge, S. Szreter, Eds. Oxford University Press, 2012.

[8] L. Lazarus, "Mapping the right to security," in *Security and human rights*, B. J. Goold, L. Lazarus, Eds. Oxford: Hart Publishing, 2007.

[9] S. Fredman, "The positive right to security," in *Security and human rights*, B. J. Goold, L. Lazarus, Eds. Oxford: Hart Publishing, 2007.

[10] A. Walsham, "The social history of the archive: Record-keeping in early modern Europe," Past & Present, vol. 230, no. suppl_11, pp. 9–48, 2016, doi: 10.1093/pastj/gtw033.

[11] M. Brosius, "Ancient archives and concepts of record-keeping: An introduction," in *Ancient archives and archival traditions: Concepts of record-keeping in the ancient world*, M. Brosius, Ed. New York: Oxford University Press, 2003.

[12] S. Simitis, "Einleitung," in *Kommentar zum Bundesdatenschutzgesetz (BDSG)*, S. Simitis, U. Dammann, O. Mallmann, H.-J. Reh, Eds. Baden-Baden: Nomos Verl.-Ges., 1978.

[13] D. Markopoulou, V. Papakonstantinou, P. de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA"s role and the General Data Protection Regulation," *Computer Law & Security Review*, vol. 35, no. 6, 2019, doi: 10.1016/j.clsr.2019.06.007.

[14] European Union. (2013). Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace, JOIN/2013/01 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001. [Accessed: Sep. 1, 2022].

[15] M. Baezner, S. Cordey. (2019, Mar. 3). *National cybersecurity strategies in comparison – Challenges for Switzerland*, Zürich: Center for Security Studies (CSS), ETH Zürich, doi: 10.3929/ethz-b-000352773.

[16] S. Dimitrova, S. Stoykov, Y. Kochev, "National cybersecurity strategies in Member States of the European Union," *ACJ*, vol. 4, no. 73, p. 54, 2015, doi: 10.17770/acj.v4i73.4355.

[17] European Union. (2020). The EU's Cybersecurity Strategy for the Digital Decade, European Commission, JOIN(2020) 18 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. [Accessed: Sep. 1, 2022].

[18] European Network and Information Security Agency. (2012, Dec. 19). *National cyber security strategies.* [Online]. Available: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementationguide. [Accessed: Sep. 1, 2022].

[19] European Network and Information Security Agency. (2016). *NCSS good practice guide: Designing and implementing national cyber security strategies*. [Online]. Available: https://data.europa.eu/doi/10.2824/48036. [Accessed: Sep. 22, 2022].

[20] European Network and Information Security Agency. (2020). *National capabilities assessment framework*. [Online]. Available: https://data.europa.eu/doi/10.2824/590072. [Accessed: Sep. 22, 2022].

[21] European Union Agency for Cybersecurity (2019). "Good practices in innovation on cybersecurity under the NCSS" [Online]. Available: https://data.europa.eu/doi/10.2824/01007. [Accessed: Sep. 22, 2022].

[22] A. Jacuch, "Comparative analysis of cybersecurity strategies", *On-line Journal Modelling the New Europe*, no. 37, p. 102, 2021, doi: 10.24193/OJMNE.2021.37.06.

[23] E. Luiijf, K. Besseling, P. de Graaf, "Nineteen national cyber security strategies," *International Journal of Critical Infrastructures*, vol. 9, no. 1–2, pp. 3–31, 2013, doi: 10.1504/IJCIS.2013.051608.

[24] G. Christou, *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Basingstoke, New York: Palgrave Macmillan, 2016.

[25] M. Dunn Cavelty. (2013). *A Resilient Europe for an open, safe and secure cyberspace*, UI Occasional papers. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368223. [Accessed: Sep. 9, 2022].

[26] C. Moorey, *A History of Crete*. London: Haus Publishing, 2019.

[27] N. Adiyeke, N. Adiyeke, E. Balta, "The Poll Tax in the years of the Cretan War: Symbol of submission and mechanisms of avoidance," *Thesaurismata*, vol. 31, pp. 323–59, 2001.

[28] V. Papakonstantinou, "Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?," *Computer Law & Security Review*, vol. 44, 2022, doi: 10.1016/j.clsr.2022.105653.