Discursive continuity and change in the time of COVID-19: The case of EU Cybersecurity Policy

Helena Carrapico

Benjamin Farrand[1]

Introduction

European Union (EU) Cybersecurity is a comparatively new field, which has moved from playing a minor supporting role in European integration to becoming its own distinct policy area in 2013. Growing from an *ad hoc* set of Single Market protection mechanisms to a fully realised agenda with its own internal rationale, cybersecurity is now central to the EU's integration efforts, with transversal effect on most other policy areas. It covers a range of activities, including the protection of critical information systems and infrastructures from cyber-attacks, the prevention and investigation of cybercrime, and cyber-defence. Similarly, in the context of the current pandemic, uses of digital communications technologies have proliferated, raising both the profile and importance of cybersecurity in supporting modern social, economic and political life. As reliance on digital communications has increased, so too have the opportunities for actors to abuse these technologies for political and economic gain.

Bearing this background in mind, this article asks whether Covid-19 has resulted in ideational change in the EU's cybersecurity policy, or whether we instead see ideational and policy continuity. For the purpose of this article, we propose that continuity involves the following three elements: 1) ideational continuity- is there a shift is the underlying philosophy and justification of EU cybersecurity policy choices?-, 2) policy continuity- is there a re-

[1] Author affiliations: Dr Helena Carrapico (corresponding Author), Associate Professor in Criminology and International Relations, Northumbria University, Department of Social Sciences, Lipman Building, Newcastle-upon-Tyne, NE18ST. E-mail: Helena.farrand-carrapico@northumbria.ac.uk Dr Benjamin Farrand, Reader in Law and Emerging Technologies, Newcastle University, Law School. Newcastle-upon-Tyne. E-mail: ben.farrand@newcastle.ac.uk

Acknowledgements: The authors would like to thank Dr Sarah Wolff and Dr Stella Ladi for their insightful and thoughtful comments to an earlier draft of this article.

orientation/ interruption of existing instruments?-, and 3) governance continuity- is the field governed in the same way, and are the relations between the different actors present in this field maintained? (for further suggestions of how to measure and analise change, please see article 1, this issue). Through an approach that draws from both historical and discursive institutionalisms, the article argues that the historical and discursive context in which EU Cybersecurity policy emerges and develops directly shapes the development of the policy itself, as well as the behaviour of actors present within the policy (Schmidt, 2008; Steinmo, 2008). By exploring the discourses at the origins of the policy, the article proposes that the development and formalisation of EU cybersecurity is the result of ideational path-dependence based in economic and security rationales that have reoriented during critical junctures. EU cybersecurity is best understood as evolving through a gradual layering of institutions and policies *and* through critical junctures, rather than exclusively as the result of either. The article concludes that while the pandemic has had a dramatic impact on daily life, it has not resulted in a significant discursive shift in cybersecurity, but rather in reinforcing existing narrative trends (for another example of policy continuity in times of Covid-19, please see article 7, this special issue).

In particular, the spread of online disinformation has resulted in a 'bifurcation' in the levels of trust placed in different actors involved in providing cybersecurity, with social media platforms deemed as not sharing the EU's values regarding freedom of expression and harmful speech, which is exacerbated by the proliferation of pandemic-related conspiracy theories. This EU cybersecurity case study aims to contribute to the historical institutionalism literature by demonstrating how it can be enriched through engagement with discursive institutionalism's focus on how ideas and discourse facilitate institutional change (for a more in-depth discussion on neo-institutionalist analytical frameworks and a defence of methodological pluralism, please see article 10, this special issue). It does so by presenting the development of EU cybersecurity through historiographical analysis, reframing the genesis, formalisation and current acceleration of EU Cybersecurity in light of the underlying philosophies that shape its programmes and policies, and identifying patterns of change and continuity.

Understanding EU Cybersecurity Policy through the lenses of historical and discursive institutionalism

In order to understand institutional change within EU cybersecurity policy, the authors propose combining the insights of historical institutionalism, in particular the elements of path dependence, critical junctures and gradual institutional change, with those of the more recent discursive institutionalism, namely the focus on the role of ideas and discourse. This section of the article explains how the discursive institutionalist analytical framework complements the historical institutionalist materialist toolbox to fully understand the ideas present at the origin and throughout the development of EU cybersecurity policy, their discursive framing, and their shaping of this policy's design and trajectory, in order to shed light onto the impact of COVID-19.

Historical institutionalism is concerned with the way institutional structures evolve over time and how this shapes their present assemblages and their surroundings (Fioretos et al., 2018). It explains institutional evolution by depicting it as the result of 'path dependence'. Current institutions are the result of past developments and policy decisions, which delimit the spectrum of current and future options (Steinmo et al., 1992). This institutional inheritance, or 'path-dependence', constrains institutional configurations and the preferences of the individuals within them (Peters, 2019). According to this view, the same exogenous phenomenon can lead to a very different impact on similar and comparable institutions due to the historical paths these institutions have taken. Institutional trajectories, however, can shift paths at specific moments in time when they reach 'critical junctures'. Defined by Collier and Collier as periods of considerable change, that may play out differently in distinct settings, critical junctures' impact on path dependence is expected to vary according to their length, timing and effect (1991). A critical juncture has the capacity to alter the trajectory of an institution by producing a new legacy in the form of novel ideas and antecedents for decision-making, which in turn will delimit future behaviour (Ladi, 2011). We argue, however, that critical junctures alone are not able to account for all forms of institutional change, gradual processes also playing an important role in understanding the evolution of EU policies (Streeck and Thelen, 2005): critical junctures serve as windows of opportunity for deeper reforms that produce path dependence, which frame the everyday micro changes that continue to take place and that equality contribute towards changing institutional trajectories, although in a less perceptible way. As the subsequent sections of this article will demonstrate, gradual changes in EU cybersecurity-related institutions are best understood through the mode of 'layering'- where new institutions are added on top of older ones (Mahoney and Thelen, 2010).

Is it possible, however, to fully understand the reasons behind institutional change by simply tracking the evolution in procedures, norms, routines and conventions? Following on the steps of Schmidt's critique of historical institutionalism (Schmidt, 2010, 2008), this article also argues that even though this approach offers important tools to comprehend how change occurs, its understanding of institutions has often tended to ignore the role of ideas and their discursive framing in contributing to that change. By overlooking ideas and their expression, historical institutionalism has in fact prioritised a materialistic and deterministic understanding of institutions, focusing on their design rather than ideational content, resulting in their representation as structures where agents' meaning constructs play a limited part. It may be possible to identify the 'path dependence' that is shaping the trajectory of EU cybersecurity policy, and it might also be possible to pinpoint critical junctures and gradual changes in this area, but if we do not uncover the ideas that constitute it, the way they are communicated, and trace their influence, we are certainly missing a key part of the answer to the puzzle. In order to counter this gap, Schmidt has proposed a fourth strain of new institutionalism, discursive institutionalism, which underlines that the discursive expression of ideas has power in itself (2008, 2002). By shaping agents' perceptions of their social, political, and economic reality, ideas[2] and discourse[3] are key to understanding how interests, values, and behaviours evolve, and why institutions change.

The analytical framework created by Schmidt for capturing the role of ideas and discourse in institutional change is therefore particularly useful to understand that critical junctures emerge as periods of change because they are discursively framed as such, and that the constraints of path dependence are the result of inherited ideas and discourses that are constantly re-interpreted in light of the contemporary context. According to Schmidt, in order to understand how ideas and discourse constitute path dependence and frame change, we need to further explore the different roles that ideas can adopt in policy-making. These can be categorised according to a three-level Matryoshka doll system, characterised by processes of ideational legacy, alignment and coherence. The first doll creates an ideational outer shell made up of

[2] For the purpose of this article, ideas are understood to mean a set of policy solutions that are embedded within a belief system and implemented by actors in decision-making positions, which directly shape policy instruments and outcomes, following the identification of policy problems and the opening of windows of opportunity for institutional change (Steinmo, 2008).

[3] The expression of these ideas, or discourse, is understood as a relational system of signifying practices aimed at a given audience, whether the discourse is written, oral, or in any other form of communicating meaning (Torfing, 1999).

'philosophies'- worldviews or ideologies- that serve as a capsule for the second doll, composed of 'programmes'- where philosophies are applied to specific policy fields and translated into underlying principles and strategic guidance. The third and most inner doll corresponds to the 'policies' that result from the practical application of philosophies and programmes (2008). This article proposes to apply this framework by identifying the implicit philosophic ideas shaping EU cybersecurity path dependence and change, in order to understand how they resulted in ideationally aligned programmes and policies, which in turn allows us to understand the impact of COVID-19 on this field.

The Origins and formalisation of EU Cybersecurity Policy

Combining historical institutionalism with discursive institutionalism, the second section of this article will now explore the emergence and formalisation of EU cybersecurity policy. It will use Schmidt's ideational categorisation in order to pinpoint this policy's foundational philosophies, tracing its discursive path dependence, and identifying the critical junctures and gradual change that have shaped programmes and policies. It proposes to sub-divide EU cybersecurity policy's path into two main phases: 1) genesis (1980 to 2010) and 2) formalisation (2010-2020). The purpose of this section is to explain that the EU cybersecurity policy's response to COVID-19, namely in terms of its relationship with the private sector, its prioritisation of resilience and combating disinformation, and the EU's coordinating role, cannot be understood as a reaction to an exogenous shock, but rather needs to be situated in a much wider ideational and discursive historical context.

Genesis: from safeguarding the Single Market to protecting EU citizens

The European Community's initial interest in cybersecurity in the 1980s was deeply embedded in an economic approach concerning Single Market protection in the context of new technologies, which would deeply influence the development of subsequent programmes and policies, and in particular, its view that cybersecurity is best governed through public-private partnerships. This security concern was reflected in international level discourses, with the Council of Europe's proposal to create the category of computer crime in the early 1980s, as well as the Organization for Economic Cooperation and Development (OECD) and the Group of Eight (G8)'s initiatives recommending the creation and harmonization of European computer crime legislation in the mid-1980s (Deflem and Shutt, 2006).

Despite the predominance of this security discourse at the international level, however, the European Community, which lacked legal competence in this field, followed a different path. Although we can observe a transfer from the international level to the European one in terms of the concern with computer and network crime, its framing was not embedded within a security philosophy but an economic one. This underlying discourse focused on the centrality of free trade and private initiative in bringing prosperity to European countries, as well as on the European Community's role in regulating the legal environment enabling healthy market competition (European Commission, 1985). Information and communication technologies were presented as both the Single Market's future, but also its Achilles' heel, as their abuse by foreign powers and individual criminals could seriously undermine economic development, distorting the functioning of the internal market (European Commission, 1993). This economic philosophy would mark the start of a path dependence that would shape the development of this area, with programmes and policies focusing on the protection of information and communication technologies as a crucial element of economic prosperity (European Commission, 1990).

As it became clear that compensatory security mechanisms and instruments were necessary to protect the open borders of the Single Market, a security discourse stemming from the development of the Justice and Home Affairs Pillar started to permeate the EU's approach to cybersecurity (Carrapico and Farrand, 2017). This spillover from the economic field to the security one opened a window of opportunity for the first critical juncture in cybersecurity's trajectory, changing the economic-focused path dependence that had been established in the early 1980s. The possibility of developing European instruments, coupled with the growing perception that computer crime constituted an emerging threat in a context of continuous uncertainty, enabled a new hybrid philosophy to surface, focusing on the role of information technologies in the facilitation of insecurity of the European Union and its citizens, and going much beyond the economic impact. The result was a hybrid economic/security discourse that would allow for security-focused concerns to shape future programmes and policies. By the mid-1990s, European institutions were already expressing a sense of urgency in addressing illegal and harmful content on the Internet (European Council, 1996), as well as the use of information technologies by organised criminals (Council of the European Union, 1997).

On the basis of this hybrid philosophy, and as an answer to the sense of urgency, there were a number of programmatic ideas, or guiding principles, developed between the late 1990s and the mid-2000s: 1) the projection of the EU as a coordinating actor that is well-placed to address transborder cybersecurity problems (European Council, 1999); 2) the need to focus on resilience as a strategy to protect information networks and infrastructures (Council of the European Union, 2005); 3) the importance of achieving coherence between EU actions and instruments in an area that is particularly diverse (European Commission, 1999); and 4) the centrality of working with the private sector given its ownership of information infrastructures and its perceived expertise (European Commission, 2001). The resulting policies included a gradually expanding network of very diverse measures, clearly working through a layering process, including the introduction of a European warning and information system (CERT), increasing research support for information technology, encouraging Member States to adopt similar cyber security norms, creating a European cybersecurity agency (ENISA), and raising the populations' awareness of cyber vulnerabilities.

Although this field has evolved through a layering process, where new ideas, norms and instruments have been gradually added on top of existing ones, with a clear path dependence shaped by a hybrid economic/ security philosophy, there has also been an important role played by external factors, including events and policy dynamics external to this specific field. Where the latter is concerned, there has been a clear relation between the development of the Third Pillar, and later on of the Area of Freedom, Security and Justice, and EU cybersecurity policy both in terms of the underlying philosophies and of spillover from other JHA policies. Policy makers' perceptions of external events have also contributed to the evolution of this policy, namely the growing number of cyber-attacks, as well as terrorist attacks where information technology played an important role. The case of the Madrid (2004) and London (2005) attacks are particularly important as they opened up the window of opportunity for the area's second critical juncture. Although there is no change at the level of the underlying philosophy, there is a very important shift in programmatic terms, justified on the basis of the level of threat, with the EU moving from a soft law approach to a much more formalised approach, characterised by binding instruments and the creation of a dedicated policy area (Fahey, 2014).

The Formalisation of EU Cybersecurity Policy

The formalisation of cybersecurity as a distinct policy domain began in 2010 with the release of the Internal Security Strategy (European Commission, 2010a). Initial proposals in the field of cybersecurity were gradualist in nature, with reforms proposed to supplement the initiatives being developed in the context of the Digital Agenda for Europe (European Commission, 2010b). This programme aimed to address the fragility of the EU's economies through measures to facilitate the creation of a 'Digital' Single Market (European Commission, 2010b, pp. 3–6). Trust and confidence in the online environment was identified as a policy problem to be addressed, yet whereas historically this was framed almost exclusively in terms of threats from cybercrime, we see a 'layering' effect as the Digital Agenda outlines that cybercrime is not only an issue of economically-driven activity, but can also be political, discursively employing the example of cyber-attacks against information systems in Estonia, Lithuania and Georgia that requires a cyber*security* approach rather than an exclusive focus on cybercrime (European Commission, 2010b, p. 16).

The Internal Security Strategy incorporated the reinforcement of existing agencies such as Europol with expanded competences in the field of cybercrime through a European Cybercrime Centre (EC3), and increased public-private partnership through ENISA to develop standards of best practice for cyber-attack resilience (European Commission, 2010a, pp. 9–10). The underlying ideational framework of the EU as coordinator, with expert-led public-private cooperation, and an emphasis on resilience and coherence of policies is evident in these documents. Rather than representing a critical juncture, it is a gradualist approach to cybersecurity policy formalisation, working within existing institutional structures to facilitate an expansion of actions, rather than radically rethinking them.

By 2013, this proposal had become a full, self-contained policy. Interestingly, the resulting Cybersecurity Strategy brought together the three former pillars of the EU in a comprehensive approach to online security issues, mimicking its pillar structure through measures intending on protecting the internal market by combating cybercrime, ensuring resilience for Network and Information Systems and Critical Information Infrastructures within the framework of cybersecurity, as well as introducing the concept of cyber-defence within the context of Common Security and Defence Policy (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013). The Cybersecurity Strategy continues this gradualist approach of layering, however, with the establishment of expanded competences for agencies such as ENISA, calls for reinforced cooperation between national

authorities, private sector online service providers and security experts, and increased coordination between the national and European levels as well as *between* the EU agencies in order to ensure coherence. In this respect, the underlying ideational framework remains consistent, with an emphasis predominantly on the importance of the EU economy with some recognition of non-economic drivers of cyber-attacks, with a continuing path-dependency based in ideas of coordination, coherence and the role of technical experts as 'problem solvers'. As a result, while we see the establishment of a standalone European Cybersecurity Strategy, this does not appear to be the result of an identifiable exogenous shock, but endogenous change as the result of accelerating and deepening trends in an environment of ideational continuity.

Ideational rupture: social media platforms, disinformation and a loss of trust

Whereas the period 2010-2016 constituted one of relative continuity, the period 2016-2019 can be considered one of ideational disruption. In April 2016, the High Representative of the Union for Foreign Affairs and Security Policy and the Commission published a Communication on Hybrid Threats (2016). The EU was framed as facing a changed threat landscape, with blurring lines between state and non-state, and economically-motivated and politically-motivated attacks. While the underlying philosophy of risk formulating the programme of resilience remains, the narrative regarding the nature of those threats is one in which the distinction between internal and external security are less meaningful, resulting in cooperation between the High Representative and the Commission becoming essential. In particular, the Joint Communication highlights that the growing risk is that malicious actors engage in combinations of economic, technological, military and diplomatic activities to undermine the stability of states and their economies 'while remaining below the threshold of formally declared warfare' (2016, p. 2).

Ideational continuity and path-dependence is apparent in the section of the Communication on cybersecurity, which emphasises coordination, coherence and resilience, with an enhanced role for national authorities cooperating with the private sector to ensure the resilience of information systems and critical information infrastructures (2016, pp. 10–12). Here, we can see that the emphasis remains on the cooperation between public and private sector experts, with no distinct change in philosophy or programme, and policies changing by means of gradualist layering; the success of ENISA and private-sector cooperation is used as legitimation basis for expanding the ENISA mandate and providing for 'market based' solutions through

the EU Cybersecurity Act (Regulation 2019/881, 2019). Under this law, cybersecurity 'experts' are brought into the regulatory sphere by providing accreditation and certification for ICT products, processes and services, based on the underlying philosophy that experts are best placed to oversee these activities.

Disinformation, however, is presented as a new form of threat, and social media as its key dissemination channel. While disinformation in itself is not a new phenomenon, it moves from a peripheral concern of the EU to take a central position in its security-focused initiatives, initially due to Russia's expansion of its disinformation campaigns from Russia and its periphery in its first and second phases to then focus on disruption and destabilisation in Europe in 2014, coinciding with its military incursion into the Ukraine (Treverton et al., 2018, p. 69). The European Council expressed a specific concern over online disinformation in this context, urging 'the High Representative, in cooperation with Member States and EU institutions, to prepare by June an action plan' (European Council, 2015, p. 4). It is here that the blending of the approaches coming from historical and discursive institutionalism becomes highly pertinent; whereas there is continuity coming from historical path-dependences concerning the role of private actors in the governance of cybersecurity based in understandings of expertise and aligned interests, we see a rupture as the result of an exogenous shock resulting from perceived information warfare waged by Russia. In terms of discursive institutionalism, this rupture creates an ideational critical juncture, in which the way these private actors are understood is subject to a divergence between those actors sharing the EU's interests (including providers of CII security solutions), and those that are deemed not to share the same interests, which include certain social media platforms.

Disinformation becomes more prominent in the Commission's security programme, as it becomes identified as being a source of rising instability in the EU, as well as presenting threats for effective policy-making in fields such as health and climate change (European Commission, 2018a). As stated by the Commission, 'disinformation erodes trust in institutions and in digital and traditional media, and harms our democracies by hampering the ability of citizens to take informed decisions' (2018a, p. 1), and social media platforms are specifically singled-out for having 'failed to act proportionately, falling short of the challenge posed by disinformation and the manipulative use of platforms' infrastructures' (2018a, p. 2). This Communication followed on almost immediately from the 'Cambridge Analytica' revelations, in which Facebook allowed for the 'harvesting' of millions of users' data. The information gathered was used by

Donald Trump's election campaign, as well as Leave.eu in the Brexit referendum campaign, in what was considered one of the biggest data breaches on record. Furthermore, Cambridge Analytica-obtained data was implicated in the development of targeted disinformation campaigns using conspiratorial ideas designed to serve the interests of these campaigns (Venturini and Rogers, 2019). While Zuckerberg acknowledged this 'breach of trust', policymakers have indicated their displeasure at the unwillingness of Facebook to effectively combat the spread of disinformation on its platform, as well as repeated refusals to attend hearings (Waterson, 2018). Zuckerberg did attend a European Parliament hearing in the wake of the Cambridge Analytica scandal, where MEPs indicated a deep scepticism regarding Zuckerberg's commitment to tackling disinformation (Madrigal, 2018). At the centre of this deepening distrust is a perception amongst actors in the EU that many of the US-based social media platforms do not share the EU's values where it comes to freedom of expression, with Zuckerberg espousing 'techno-libertarian' ideals and stating to the European Parliament that Facebook should not regulate what is true or not, representing a philosophical ideal that all political speech should be permitted with a plurality of views being represented (Lischka, 2019). A particularly virulent form of disinformation being spread through Facebook, ostensibly on the basis of plurality of opinion is that of 'anti-vaxxers', who criticise (often on the basis of conspiracy theories and misrepresented scientific studies) contemporary vaccination programmes, which has been linked to the increased transmission of diseases such as measles (Hoffman et al., 2019). This approach to speech is not perceived as conforming to EU principles of expression, in which speech that is considered to be actively harmful, such as hate speech or glorification of terrorism is explicitly illegal and should be actively regulated (see for example Ross, 2019). This perception resulted in the Commission's decision to propose a Regulation requiring social media to remove material deemed to constitute dissemination of materials promoting terrorism (European Commission, 2018b).

We increasingly see, as a result of this change in trust relationship, a corresponding change in underlying philosophy regarding the relationship between public and private actors, which impact upon programme and policy-level ideas. The EU's perceptions of democracy and the role of private actors within it is subject to a reorientation; whereas some private actors are trusted partners in cybersecurity, and believed to share the values of the EU, social media platforms are increasingly framed as being part of the problem, with their private sector operators not sharing those same values. At the policy level, this becomes reflected in a discourse that no longer places these platforms at the heart of policymaking as with other

cybersecurity 'experts', but rather as agents to be regulated through a Commission-developed Code of Practice for tackling disinformation in the online environment (European Commission, 2018c). In 2019, the Commission is explicit in stating that in 2020 it would conduct a review into the effectiveness of social media platforms in applying the Code of Practice, and should it find compliance unsatisfactory, it would consider alternative means of tackling this policy problem, including regulatory oversight (2019). In this respect, therefore, ideational change can be identified in how private actors are distinguished; those that are trusted, and take part in the governance network, and those that are less trusted, and as a result are no longer part of that network but instead *subject* to regulatory oversight by it.

Digital technologies have taken a preeminent policy position under the new Commission Presidency, with one stream of the Commission's agenda named Shaping Europe's Digital Future (European Commission, 2020a). The section of the document focused on cybersecurity represents the existing trends identified previously and in line with the dominant ideational philosophy, in which the necessity of tackling risks and the expertise of the private sector are present; the programme proposed is one of expanding the marketisation of cybersecurity products and creation of a single market for cybersecurity, with engagement with private sector experts and the establishment of a joint Cybersecurity Unit in order to facilitate cohesion and coordination (2020a, p. 4). This ideational path-dependence and continuity is also demonstrated in policy programmes associated with this agenda, including the European Strategy for Data (European Commission, 2020b) and New Industrial Strategy for Europe, which proposes increased private sector engagement in cybersecurity rules for 5G (European Commission, 2020c). The White Paper on Artificial Intelligence contains a section on the use of AI in the context of cybersecurity, reiterating the importance of public-private cooperation between AI experts and ENISA in this field, and the possibility of new cybersecurity products arising from developments of these technologies (European Commission, 2020d). Disinformation is not, however, mentioned within the context of the Data or Industrial Strategy documents. Instead, disinformation is framed differently in Shaping Europe's Digital Future, where emphasis is placed on the risk posed to *democracy* from disinformation and the need for transparency regarding information manipulation online, with the Commission proposing a Democracy Action Plan (2020a, p. 6). Whereas attacks on information systems and critical information infrastructure are presented as being cybersecurity threats, disinformation and information manipulation on those systems is presented as not only a cybersecurity threat but

a threat to the EU's fundamental order and values. As will be discussed in the next section, these are ideas that have been reinforced, rather than challenged, by the current pandemic.

The Impact of Covid-19 in the trajectory of EU cybersecurity policy: reinforcing of existing trends

In this final section of the article, it will be demonstrated that prior to the COVID-19 outbreak, the trends established in the period 2016-2019 are not subject to an ideational challenge, but instead COVID serves to reinforce the existing ideational path-dependency. The philosophical framework in cybersecurity, incorporating elements concerning private sector expertise and the positive nature of integration, remained consistent. However, at the programme level, while some private sector experts are considered best-placed to facilitate cybersecurity as a means of combating online risks, the operators of social media platforms are no longer considered to share the same world view as the EU on the necessity of tackling disinformation. After the COVID-19 outbreak, these trends have continued, albeit at an accelerated pace. This suggests that the underlying philosophy and programme level understanding that all private sector experts shared similar values to the EU in the field of cybersecurity was effectively challenged and had lasting effects. Indeed, there are now two discursive path-dependencies in operation, one in which the private sector providing cybersecurity is a trusted partner in governing cyberspace, and one in which social media platforms pose a challenge to the EU's security through an unwillingness or inability to effectively tackle disinformation, and thus need more oversight.

COVID-19 has dominated much of the EU's programme and policy focus in a very short time. By the end of February, the pandemic visibly emerged as *the* crisis on the EU's agenda (Council of the European Union, 2020a). Prior to the outbreak, less than 10% of workers in the EU worked from home on a daily basis (with the UK and France having approximately 12% and 17% of workers working from home), increasing to 38% by April 2020, including more than half the working population in Belgium, the Netherlands, Luxembourg, Finland and the UK (Eurofound, 2020). This increase in home-working has been seen as an opportunity for criminal actors online, with Europol reporting a significant increase in attacks on information systems, online scams and ransomware attacks (2020). Similarly, disinformation concerning the origins of COVID-19, its effects, the response of world governments and indeed the very existence of the virus began to spread from January onwards (Lovari, 2020). In April 2020, the Commission

published a Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis (Commission Recommendation 2020/518, 2020). This Recommendation specified that effective cybersecurity measures would be essential to ensure the protection of data used to tackle the crisis, including test-and-trace data. Within this Recommendation, the private sector providers of these technologies are trusted to ensure the resilience of their systems from data breaches or unauthorised access, in cooperation with data protection and health authorities.

Discursively, these private sector actors are part of the cybersecurity governance framework, with philosophical and programme level continuity, and policy change taking a gradualist layering approach. This theme continues in the 'Repair and Prepare' policy initiative proposed by the Commission in May (European Commission, 2020e), which covered a range of different activities to boost economic recovery post-COVID. In the field of cybersecurity, private sector actors are presented as contributing both to the security of the online environment in Europe, with discussion of their involvement in an expanded critical infrastructure protection initiative, as well as being a source of potential recovery through the establishment of cybersecurity-oriented Small and Medium-sized Enterprises (2020e, p. 9). At the time of writing, the most recent publication with a cybersecurity dimension is the Council Conclusions on the Shaping Europe's Digital Future agenda (Council of the European Union, 2020b). These Conclusions stress that cybersecurity is an essential contribution to the economy and safety of the EU based on principles of resilience and public-private cooperation, encouraging a continuation and expansion of these activities, agreeing that 'acceleration of the digital transformation will be an essential component of the EU's response to the economic crisis generated by the COVID-19 pandemic' (2020b, p. 2).

Responses to disinformation have reinforced the EU's perception that social media platforms do not share the same values or philosophy regarding this divisive form of communication. The Council's COVID-19 risk mitigation strategy emphasised that one necessary policy response concerned efforts intended to prevent the spread of disinformation concerning the virus (Council of the European Union, 2020a, p. 6). This is reiterated in the Commission and High Representative's Communication on the Global EU response to COVID-19, where disinformation concerning the virus is discursively framed as a threat to the EU's fundamental values and to its health security (2020a). According to Europol, disinformation concerning the outbreak and response to COVID-19 has spread rapidly since the initial outbreak in Wuhan,

with alleged sources including foreign governments, state-backed actors, political opportunists and criminal organisations (2020). In May, the Commission referred to an 'infodemic' in which false messages, often with a propaganda or hate-based narrative, was being spread. This disinformation was framed as being a threat to public health and democracy, with a need for immediate action (2020e, p. 15).

The divergent approach to social media platforms is reinforced in the Council Conclusions. Here, online platform providers are categorised separately from 'experts' and 'national authorities', with these platforms being presented as part of the disinformation threat, and the subject of demands 'for greater transparency and responsibility' (2020c). The Commission and High Representative quickly followed the Council Conclusions with a Joint Communication on tackling COVID-19 disinformation, which again reiterated the nature of disinformation as a significant threat to health and democracy. While it states that it is the requirement of a range of actors including national authorities, journalists, fact-checkers and platform operators to cooperate to identify and tackle disinformation, the narrative concerning platforms is that 'platforms have not sufficiently empowered [fact-checkers] during the current public health crisis […] there is therefore a need for additional efforts and information sharing, as well as increased transparency and greater accountability' (2020b, p. 8). The policy proposals in this area require renewed efforts by platforms to work with national authorities and fact-checkers to identify disinformation and its sources, as well as disclosing manipulative behaviour being conducted through their platforms (2020b, p. 9). In its assessment of the spread of disinformation, the EEAS noted that while social media platforms had some success in tackling disinformation regarding the virus, 'platforms are still vulnerable to being the tool for viral distribution of false information […and] this shows that further and continued efforts by the platforms are necessary beyond the Code of Practice' (EEAS, 2020). Furthermore, at the release of the Joint Communication, Commission Vice-President for Values and Transparency Vera Jourova stated that 'while online platforms have taken positive steps during the pandemic, they need to step up their efforts […] For instance we know only as much as platforms tell us — this is not good enough. They have to open up and offer more evidence' (as cited in Lomas, 2020). It is not unforeseen that the acceleration of the EU's disinformation programme may ultimately lead to a policy of increased regulation of social media, rather than the distinct 'market-based' approach being applied to actors in other fields of cybersecurity.

At the heart of the divergence in the underlying philosophy and resulting programme and policy-level responses of the EU in the field of cybersecurity is the changing understanding of the role of private actors in governance. Ultimately, it is due to the trust invested in those actors – within the ordoliberal philosophic framework, the private sector expert is an active participant in the governance of various policy areas in cooperation with EU and national authorities, with the EU best-placed to coordinate action in a cohesive and coherent manner. In most domains of cybersecurity, the private sector can be trusted to form an effective part of that network and thus contribute to the effective security and economic development of the EU, resulting in no significant challenge to the path-dependencies that have developed since the origins and formalisation of EU cybersecurity. For this reason, in most cybersecurity domains, change is of a gradual, layering nature. However, the critical juncture that has served to reorient this ideational path-dependency was not that of the financial crisis, or even that of the current pandemic. Instead, the loss of trust in certain online actors, namely social media platforms, is the result of upheavals and global instability (with 2016 being a critical year in this changing perception) that EU policymakers consider social media platforms contributed to and refuse to accept responsibility for. It is here that we see discursive change, with programme and policy level shifts concerning the role of social media platforms in tackling disinformation. While all private sector actors can contribute to providing security and economic growth to the EU, some are more trusted to do so in line with the EU's fundamental values than others.

Conclusion

By reframing the development of EU Cybersecurity through the lenses of historical and discursive institutionalism, it has been possible to identify the key ideas that have produced discursive path-dependencies in this field. Just as importantly, by using this approach, it has been possible to better understand the conditions in which ideational path-dependency in institutions continues or changes, and how this can impact upon programme and policy-level narratives. In the field of cybersecurity, while critical junctures have served to facilitate change in underlying ideas that shape programmes and policies, they are not necessarily the critical junctures that may be expected. Whereas the spread of COVID-19 has been highly destabilising to economies, societies and the daily life of public and private actors, it does not appear to have served in itself as a critical juncture in the EU's understanding of cybersecurity. Instead, the pandemic has resulted in the existing ideational position that social media providers, rather than contributing to effective cybersecurity, are in fact hindering it. Perceiving them as both a

form of hybrid cybersecurity threat, as well as representing a broader threat to the EU's democratic values, the EU's position on social media platforms was shaped by an earlier critical juncture, in 2016. During this juncture, the discourse concerning the role of these platforms in the digital environment was subject to a rhetorical change underlining their role in the dissemination of disinformation. The increased spread of disinformation concerning COVID-19 in 2020 has provided a basis for policy continuity rather than rupture, reinforcing the concerns regarding the role of these platforms as a source of insecurity, in comparison to private providers of cybersecurity solutions, which are deemed to share the interests and values of the EU. The rise in cyber-attacks and increased spread of disinformation during the pandemic, particularly concerning the nature of the disease and its origins, has therefore not resulted in a significant shift in the EU's thinking in this field, but instead reinforced its existing perceptions regarding the roles of different security providers, and therefore served to ensure ideational continuity in its existing policy approaches rather than result in a change in them.

More generally, this article highlights that events that on their surface appear to 'change everything', whether the realisation of mass consumer use of the Internet in the late 1990s, or indeed the pandemic of 2020, must be carefully assessed in terms of the changes they truly instil. While there may be far-reaching and long-standing changes to aspects of EU policymaking in fields such as health or migration, as we seek to better understand and control the aspects of pandemic response that relate to the treatment and movement of people that may be infected with a novel coronavirus, in the field of cybersecurity, we do not see the same dramatic change in policies, but instead, a reinforcing of existing ideas and attitudes, albeit with a renewed impetus and an acceleration of action. The disinformation, and social media's role in its spread, are not new and not unexpected. Instead, the inability or unwillingness of social media to effectively suppress it has resulted in a confirmation of the pre-existing ideational position of the Commission, resulting in policy announcements that pursue previously stated goals rather than constituting a dramatic change.

References

Carrapico, H., Farrand, B., 2017. 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. Crime Law Soc. Change 67, 245–263.

Collier, R.B., Collier, D., 1991. Shaping the Political Arena: Critical Junctures, the Labor Movement, and Regime Dynamics in Latin America. Princeton University Press, Princeton, N.J.

Commission Recommendation 2020/518, 2020. on a common Union toolbox for the use of technology and data to combat and exit from the COVID- 19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.

Council of the European Union, 2020a. Council Conclusions on COVID-19 (No. OJ C 57/4).

Council of the European Union, 2020b. Council conclusions on shaping Europe's digital future (No. OJ 2020C 202).

Council of the European Union, 2020c. Council conclusions on media literacy in an ever-changing world (No. OJ C 193).

Council of the European Union, 2005. Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems (No. L 69/67), Official Journal of the European Union.

Council of the European Union, 1997. Action Plan to Combat Organised Crime (No. No C251/1-15.8.97), Official Journal of the European Communities. Brussels.

Deflem, M., Shutt, E., 2006. Law Enforcement and Computer Security Threats and Measures, in: Bidgodi, H. (Ed.), Handbook of Information Security, Information Warfare, Social, Legal, and International Issues, and Security Foundations. John Wiley & Sons, Inc., pp. 200–209.

EEAS, 2020. Short assessment of narratives and disinformation around the Covid-19 pandemic (Updat 23 April – 18 May) [WWW Document]. EU Vs DISINFORMATION. URL https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may/ (accessed 8.30.20).

Eurofound, 2020. Work, teleworking and COVID-19 [WWW Document]. Eurofound. URL https://www.eurofound.europa.eu/data/covid-19/working-teleworking (accessed 8.22.20).

European Commission, 2020a. Shaping Europe's Digital Future.

European Commission, 2020b. A European strategy for data (No. COM(2020) 66).

European Commission, 2020c. A New Industrial Strategy for Europe (No. COM(2020) 102 final).

European Commission, 2020d. White Paper on Artificial Intelligence: A European approach to excellence and trust (No. COM(2020) 65).

European Commission, 2020e. Europe's moment: Repair and Prepare for the Next Generation (No. COM(2020) 456 final).

European Commission, 2019. Code of Practice on Disinformation: First Annual Reports.

European Commission, 2018a. Tackling online disinformation: a European Approach (No. COM(2018) 236).

European Commission, 2018b. Proposal for a Regulation on preventing the dissemination of terrorist content online (No. COM(2018) 640 final).

European Commission, 2018c. EU Code of Practice on Online Disinformation.

European Commission, 2010a. The EU Internal Security Strategy in Action: five steps towards a more secure Europe (No. COM(2010) 673 final).
European Commission, 2010b. A Digital Agenda for Europe (No. COM(2010) 245 final/2). Brussels.
European Commission, 2001. Network and Information Security: Proposal for A European Policy Approach (No. COM(2001) 298 final). Brussels.
European Commission, 1999. E-Europe- An Information Society for All. Communication on a Commission Initiative for the Special European Council of Lisbon (No. COM(1999) 687 final).
European Commission, 1993. Growth, Competitiveness, Employment: the Challenges and Ways Forward into the 21st Century- White Paper (No. COM(93)700 final).
European Commission, 1990. Proposal for a Council Decision in the Field of Information Security (No. COM(90) 314 final-SYN288).
European Commission, 1985. White Paper: Completing the Internal Market (No. COM(85) 310 final). European Commission, Brussels.
European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020a. Communication on the Global EU response to COVID-19 (No. JOIN(2020) 11 final).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020b. Tackling COVID-19 disinformation - Getting the facts right (No. JOIN(2020) 8 final).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016. Joint Framework on countering hybrid threats (No. JOIN(2016) 18).
European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (No. JOIN(2013) 1). Brussels.
European Council, 2015. Council Conclusions (No. EUCO 11/15, CO EUR 1, CONCL 1).
European Council, 1999. Council Conclusions. Tampere.
European Council, 1996. Council presidency conclusions (No. December). Dublin.
Europol, 2020. Catching the virus: cybercrime, disinformation and the COVID-19 pandemic.
Fahey, E., 2014. The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. Eur. J. Risk Regul. EJRR 5, 46.
Fioretos, O., Falleti, T.G., Sheingate, A., 2018. Historical Institutionalism in Political Science, in: Fioretos, O., Falleti, T.G., Sheingate, A. (Eds.), The Oxford Handbook of Historical Institutionalism. Oxford.
Hoffman, B.L., Felter, E.M., Chu, K.-H., Shensa, A., Hermann, C., Wolynn, T., Williams, D., Primack, B.A., 2019. It's not all about autism: The emerging landscape of anti-vaccination sentiment on Facebook. Vaccine 37, 2216–2223. https://doi.org/10.1016/j.vaccine.2019.03.003
Ladi, S., 2011. Think Tanks, Discoursive Institutionalism and Policy Change, in: Papanagnou, G. (Ed.), Social Science and Policy Challenges- Democracy, Values and Capacities, Research and Policy. UNESCO Publishing, Paris, pp. 205–220.
Lischka, J.A., 2019. Strategic Communication as Discursive Institutional Work: A Critical Discourse Analysis of Mark Zuckerberg's Legitimacy Talk at the European Parliament. Int. J. Strateg. Commun. 13, 197–213. https://doi.org/10.1080/1553118X.2019.1613661

Lomas, N., 2020. Tech giants must open up about the coronavirus 'infodemic', say EU lawmakers. TechCrunch. URL https://social.techcrunch.com/2020/06/10/tech-giants-must-open-up-about-the-coronavirus-infodemic-say-eu-lawmakers/ (accessed 8.30.20).

Lovari, A., 2020. Spreading (Dis)Trust: Covid-19 Misinformation and Government Intervention in Italy. Media Commun. 8, 458–461. https://doi.org/10.17645/mac.v8i2.3219

Madrigal, A.C., 2018. A Belgian Legislator Berates and Scoffs at Mark Zuckerberg [WWW Document]. The Atlantic. URL https://www.theatlantic.com/technology/archive/2018/05/a-belgian-legislator-berates-and-scoffs-at-mark-zuckerberg/560960/ (accessed 8.28.20).

Mahoney, J., Thelen, K. (Eds.), 2010. Explaining Institutional Change: Ambiguity, Agency, and Power, Illustrated edition. ed. Cambridge University Press, Cambridge ; New York.

Peters, B.G., 2019. Institutional Theory in Political Science, Fourth Edition: The New Institutionalism, 4 edition. ed. Edward Elgar Publishing Ltd, Northampton, MA.

Regulation 2019/881, 2019. on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

Ross, A., 2019. Values and Issues, in: Ross, A. (Ed.), Finding Political Identities: Young People in a Changing Europe, Palgrave Politics of Identity and Citizenship Series. Springer International Publishing, Cham, pp. 45–95. https://doi.org/10.1007/978-3-319-90875-5_2

Schmidt, V.A., 2010. Reconciling Ideas and Institutions through Discursive Institutionalism, in: Beland, D., Cox, R.H. (Eds.), Ideas and Politics in Social Science Research. Oxford University Press, Oxford, England ; New York.

Schmidt, V.A., 2008. Discursive Institutionalism: The Explanatory Power of Ideas and Discourse. Annu. Rev. Polit. Sci. 11, 303–326. https://doi.org/10.1146/annurev.polisci.11.060606.135342

Schmidt, V.A., 2002. Does Discourse Matter in the Politics of Welfare State Adjustment? Comp. Polit. Stud. 35, 168–193. https://doi.org/10.1177/0010414002035002002

Smith, N., Graham, T., 2019. Mapping the anti-vaccination movement on Facebook. Inf. Commun. Soc. 22, 1310–1327. https://doi.org/10.1080/1369118X.2017.1418406

Steinmo, S., 2008. What is Historical Institutionalism?, in: Della Porta, D., Keating, M. (Eds.), Approaches in the Social Sciences. Cambridge University Press, Cambridge, pp. 118–138.

Steinmo, S., Thelen, K., Longstreth, F. (Eds.), 1992. Structuring Politics: Historical Institutionalism in Comparative Analysis. Cambridge University Press, Cambridge England ; New York.

Streeck, W., Thelen, K.A., 2005. Beyond Continuity: Institutional Change in Advanced Political Economies. Oxford University Press.

Torfing, J., 1999. New Theories of Discourse: Laclau, Mouffe and Zizek. Blackwell Publishers, Oxford.

Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., McCue, M., 2018. Addressing Hybrid Threats. Center for Asymmetric Threat Studies; The European Centre of Excellence for Countering Hybrid Threats, Swedish Defence University.

Venturini, T., Rogers, R., 2019. "API-Based Research" or How can Digital Sociology and Journalism Studies Learn from the Facebook and Cambridge Analytica Data Breach. Digit. Journal. 7, 532–540. https://doi.org/10.1080/21670811.2019.1591927

Waterson, J., 2018. Five things we learned from Mark Zuckerberg's European parliament appearance. The Guardian.