The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market?[1]

Política de ciberseguridad de la Unión Europea (UE): ¿narrativa estratégica propia de una ciber potencia o discurso ambiguo para el mercado común?

Agnes Kasper
Tallinn University of Technology, Estonia
agnes.kasper@taltech.ee

Vlad Vernygora
University of Lapland, Finland
vvernygo@ulapland.fi

doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71

Recibido el 20 de noviembre de 2020
Aceptado el 18 de mayo de 2021

Abstract: In the last decade, cybersecurity has swiftly turned into a strategic issue and became an important horizontal policy area in the EU, which is treated in this article as one of the four contemporary political empires. These days, the policy arguably encompasses both internal and external aspects, often making it difficult to assess the level of its actual effectiveness as well as outreach. Initially, the EU's introverted vision on the issue drove the policy to focus on cyber resilience and strategic autonomy. Evidently, the EU's strategic narrative that could assist it in leading the process of creating an open, free, stable and secure cyberspace in the digital decade, in the context

---

[1] This work was carried out with the support of the Erasmus+ programme of the European Union, CASPA Project (Erasmus+ 2020-1-EE01-KA203-077958). The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein.

of international security, is emerging. Thus, this contribution is to test the argument that the EU, utilizing an imperial paradigm (consciously or not), is gradually becoming a global steering power in cybersecurity. In this article, firstly, we identify and examine the process of formation of the EU's narratives about (its) cyber power. Secondly, we establish a discussion framework to highlight the methodological relevance of the imperial paradigm, cyber power Europe and Strategic Narrative Theory for a multidisciplinary debate on global geo-strategic redesign, in which the EU takes part. Thirdly, we look into bilateral and multilateral forums and processes that deal with cybersecurity and in which the EU participates, in order to understand more specifically how the EU is projecting its cyber-power narratives internationally and how cybersecurity-associated challenges impact current dynamics in other policy domains in the field of international relations.

Keywords: Cybersecurity, Strategic Narrative Theory, EU Strategic Narratives, Cyber Power Europe, Cyber "Maastricht", Contemporary Empires.

Resumen: *En la última década, la ciberseguridad se ha convertido en asunto estratégico y del ámbito político horizontal de la UE, Unión que este artículo considera uno de los cuatro imperios políticos contemporáneos. Cabe afirmar que hoy en día la política abarca asuntos internos y externos, lo cual a menudo dificulta estimar su eficacia y alcance con precisión. La introversión de la UE sobre el tema le llevó en un principio a centrarse en la ciber-resiliencia y la autonomía estratégica. Sin embargo, en el contexto de la seguridad internacional, se ha hecho evidente que la EU comienza a desarrollar una narrativa estratégica que podría ayudarle a liderar la creación de un ciberespacio abierto, libre, estable y seguro para la década digital. Por tanto, este escrito examina si la UE, utilizando un paradigma imperial (conscientemente o no), se ha ido constituyendo gradualmente en una potencia de ciberseguridad global. Para comenzar, identificamos y estudiamos el proceso de formación de las narrativas de la UE sobre (su) poder cibernético. En segundo lugar, establecemos un marco de discusión, resaltando la relevancia metodológica que tienen para el debate multidisciplinario sobre el reordenamiento geo-estratégico mundial, en el que participa la UE, el paradigma imperial de la ciber-potencia Europa, y la Teoría de la Narrativa Estratégica. Por último, analizamos los foros y actividades bilaterales y multilaterales que se ocupan de la ciberseguridad y en los que la UE toma parte, con el fin de aclarar la forma en que proyecta sus narrativas como poder cibernético a nivel internacional, y el modo en que los desafíos asociados a la ciberseguridad afectan las dinámicas actuales de otros ámbitos políticos en el campo de las relaciones internacionales.*

Palabras clave: *ciberseguridad, Teoría de la Narrativa Estratégica, narrativas estratégicas de la UE, Ciber-potencia Europa, Ciber "Maastricht", Imperios contemporáneos.*

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

I. **Introduction**

Cybersecurity and communication are processes with inherent potential for yielding power. The European Union (EU) is evidently engaged in doing both, gradually building its cyber powers and issuing both strategic and other messages for the global audience to react to. However, considering the EU's real and perceived leverage in the field of international relations, these processes are not conducted for nothing but, most definitely, for the benefit of steering the entity towards reaching its tactical and strategic goals. In this research, generally, we make an attempt to dot the *i*'s and cross the *t*'s on those messages that the EU formulates about its cyber powers, underlining the entity's non-conventional status in the current international system. For the purposes of the analysis, we focus on the policy statements, official communications (or lack thereof) and also publicly available internal documents of the EU related to dimensions of cyber power in the EU's context. On a more concrete note, this contribution is visualised to complete a "sequel", which was commenced by our previously published research on the EU and its stance on cybersecurity.[2] We have explored the theoretical foundations of the policy utilizing the toolboxes of neofunctionalism, liberal intergovernmentalism, post-functionalism and the imperial paradigm to construct a "Cyber Maastricht" model, based on the pillars of "Resilience", "Deterrence", and "Defence & International Relations".[3]

Building on this earlier research, this article considers whether there is a conceptual interlinkage between the EU's evident status of a contemporary political empire[4] with a global mission, its detectable capabilities of being a cyber power, and the entity's declared as well as strategic plan on leading the process of strengthening international cooperation in cyberspace.[5] Structurally, this article firstly identifies and

---

[2] Agnes Kasper and Vlad A. Vernygora, "Towards a 'Cyber Maastricht': Two Steps Forward, One Step Back," in *The Future of the European Union: Demisting the Debate*, eds. Mark Harwood, Stefano Moncada, and Roderick Pace (Msida: Institute for European Studies, 2020), 186-210.

[3] Kasper and Vernygora, 202-205.

[4] Jan Zielonka, *Europe as Empire. The Nature of the Enlarged European Union* (Oxford: Oxford University Press, 2006); Noel Parker, "Theoretical Introduction: Spaces, Centers, and Margins," in *The Geopolitics of Europe's Identity: Centers, Boundaries, and Margins*, ed. Noel Parker (New York: Palgrave, 2008), 3-23; Magali Gravier, "The Next European Empire?" *European Societies* 4, no.5 (2009), 627-647.

[5] High Representative of the European Union for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (JOIN (2013) 1 final, Brussels 2013).

examines EU-originated plans and actions on cybersecurity through the prism of the entity's strategic narratives about (its own) cyber powers, which, adopting Klimburg's Integrated Capability Model,[6] are measurable in principle. There is an assumption here that the EU has at least some abilities to shape the world's cybersecurity landscape, interlinking its activities with the process of constructing its strategic identity, system, and policy narratives, which can also be identified.

Secondly, the discussion highlights the methodological relevance of the Strategic Narrative Theory's postulates[7] and the theory-associated analytical instrumentarium for a multidisciplinary debate on global geo-strategic redesign. For the EU, such a debate is of immense importance, since the entity, despite being increasingly treated as a contemporary empire, represents a non-conventional member of the United Nations (UN)-based international system. Whatever the latter can be symbolised by, but, arguably, it cannot be symbolised by what Hardt and Negri called "a single logic of rule"[8] as being *fait accompli*. Such a state of affairs cannot be detected at present, but it can be described as a desirable point of geo-strategic "arrival" for the EU (as well as China, Russia, and the United States).

Thirdly, before discussing the findings and then concluding, this contribution examines bilateral and multilateral *fora* which focus on cybersecurity, and in which the EU directly participates, projecting (even if unintentionally) its cyber-power strategic narratives globally (and, more specifically, to the Asia-Pacific region). The process of strategising the EU's communication with the world on the issue of cybersecurity has already begun, and this contribution is among the first to analytically detect and highlight the emergence of a new multi-faceted strategic narrative within the EU that has to now focus more on leading global engagement and, most probably, providing a unifying functional platform for cooperation on the issue. The EU's identity, system and policy narratives on the three dimensions of (its) cyber power are presented in *Table 2*. in the last chapter.

---

[6] Alexander Klimburg, "The Whole of Nation in Cyberpower," *International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity*, a Special issue of *Georgetown Journal of International Affairs* (Georgetown University Press, 2011), 171-179.

[7] Alister Miskimmon, Ben O'Loughlin, and Laura Roselle, *Strategic Narratives: Communication Power and the New World Order* (New York, London: Routledge, 2013); Laura Roselle, Alister Miskimmon, and Ben O'Loughlin, "Strategic Narrative: A New Means to Understand Soft Power," *Media, War & Conflict* 7, no.1 (2014), 70-84.

[8] Michael Hardt and Antonio Negri, *Empire* (Cambridge, MA: Harvard University Press, 2000), xii.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

II. **The EU and its actions on cybersecurity**

1. *Policy landscape: cyber everywhere*

The EU has portrayed itself as a "force for good" that promotes respect for personal freedom, human dignity, solidarity, market economics, democracy and the rule of law, although the pre-eminence of its own norms is also implied in its interactions with others.[9] Continuing the implementation of its ambitious plan on the Digital Single Market, where cybersecurity is an enabling factor, the EU is now engaged in 'Shaping Europe's Digital Future'[10] using its economic power, coordinative functions and normative appeals. The strategy boldly emphasises the importance of the external dimension in this context and observes that the EU-originated model has become an inspiration globally and "[m]any countries around the world have aligned their own legislation with the EU's strong data protection regime",[11] all of which leads to the overt aim of the EU becoming a digital regulatory superpower. However, one may claim that this can only be a possibility if the EU manages to explicitly formulate its conceptual understanding of what strategic autonomy really means for the entity to eventually become a true digital superpower in its own right.

Cybersecurity is a cross-cutting issue in the European Commission's action plans and it features in the EU's data[12] and artificial intelligence strategies,[13] in the new industrial strategy,[14] SME strategy,[15] "A Global Strategy for the European Union's Foreign and Security Policy",[16] and in the updated Cyber Defence Policy Framework.[17] While the above illustrates well how a comprehensive multi-dimensional cybersecurity

---

[9] Cristian Nițoiu, "The Narrative Construction of the European Union," *External Relations, Perspectives on European Politics and Society* 14, no.2 (2013), 247 (240-255).

[10] European Commission, "Shaping Europe's Digital Future" (COM (2020) 67 final, Brussels, 2020c).

[11] European Commission, 2020c.

[12] European Commission, "A European Strategy for Data" (COM (2020), 66 final, Brussels, 2020b).

[13] European Commission, White Paper, "On Artificial Intelligence – A European Approach to Excellence and Trust" (COM (2020), 65 final, Brussels, 2020a).

[14] European Commission, "A New Industrial Strategy for Europe" (COM (2020) 102 final, Brussels, 2020d).

[15] European Commission, "An SME Strategy for a Sustainable and Digital Europe" (COM (2020) 103 final, Brussels, 2020e).

[16] European External Action Service, "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy" (Brussels, 2016).

[17] Council, "EU Cyber Defence Policy Framework" (14413/18, Brussels, 2018d).

approach looks, this should not be mistaken for an integrated approach. The EU's 2017 Cybersecurity Strategy[18] makes it clear that the primary responsibility in this policy area rests with individual Member States and that the EU's role is supportive, coordinative and advisory.[19] While this approach, internally, raises problems on its own, the actual challenge is much greater since the EU continues to struggle with issues of strategic autonomy and technological sovereignty in its external relations. However, the new 2020 EU's Cybersecurity Strategy for the Digital Decade[20] reflects an ambitious plan on increasing coherence within the policy and with other policy areas, distinctly setting the tone for the EU's engagement with the rest of the world, demonstrating its cyber powers, and defining a non-military, but unyielding approach to cybersecurity.

2. *EU's cybersecurity policy*

In noticeable details, the cybersecurity policy of the EU began to emerge from the mid-1990s, originally focusing only on specific areas such as telecommunications and personal data protection. Normatively, the EU was also keeping an eye on and following the emergence of the 2001 Council of Europe (CoE) Convention on Cybercrime,[21] while its competences in areas relating to criminal matters were evolving under the Area of Freedom, Security and Justice that was formally established in 1999.[22] The 9/11 terrorist attacks prompted more attention to the security of critical infrastructures, and several EU-level initiatives addressing the security of their underlying information systems and networks testified to the increasing concern about the new challenges technological

[18] European Commission, "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU" (JOIN (2017), 450 final, Brussels, 2017).

[19] Agnes Kasper and Holger Mölder, "The EU's Common Security and Defence Policy in Facing New Security Challenges and Its Impact on Cyberdefence," in *The EU in the 21st century. Challenges and Opportunities for the European Integration Process*, eds. David Ramiro Troitiño, Tanel Kerikmäe, Ricardo Martín De la Guardia, and Guillermo Á Pérez Sánchez (Springer, 2020), 291 (271-294).

[20] European Commission, "EU Security Union Strategy" (COM (2020) 605 final, Brussels, 2020j).

[21] Council of Europe, "Convention on Cybercrime" (ETS No. 185, Budapest, 2001).

[22] Nataliia Oliievska, David Ramiro Troitiño, and Tanel Kerikmäe, "Internal Security: Terrorism and Criminality Fostering Integration in the EU," in *The EU in the 21st century. Challenges and Opportunities for the European Integration Process*, eds. David Ramiro Troitiño, Tanel Kerikmäe, Ricardo Martín De la Guardia, and Guillermo Á. Pérez Sánchez (Springer, 2020), 86 (85-100).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

developments bring. Yet, it took until 2008 when cybersecurity clearly arose as a serious strategic issue.[23]

The EU's 2013 Cybersecurity Strategy[24] defined the main priority areas and direction for further efforts, and had a strong focus on addressing threats emanating from the economic sphere. However, the document's revised version in 2017 had a palpable political and defence undertone added to the scheme of actions, pointing towards cyber threat vectors as both state and non-state actors: "they are often criminal, motivated by profit, but they can also be political and strategic".[25] The intensification of discussions and focus on politically sensitive issues came as no surprise, but rather as a natural process in pursuit of the implementation of the 2013 Strategy. Since that point, the EU had made its first significant steps towards cyber defence cooperation, adopting the first EU cyber defence policy framework in 2014,[26] updated in 2018.[27] Also, as a result of continued reflections on state-sponsored cyber attacks and other consequential problems, the proposal for the development of joint EU diplomatic responses against coercive cyber operations was tabled in 2016 in the Council of the EU,[28] leading to the adoption of the EU Cyber Diplomacy Toolbox in 2017[29] and clearly indicating the strong external element in the overall cybersecurity policy of the EU. The 2020 Cybersecurity Strategy for the Digital Decade[30] goes even further, addressing political and military threats and devising a more integrated and, in many respects, externally expansive policy, while also aiming to shield the EU from external dependencies and threats. This approach is exhibited in the title of the Strategy's second part: "Thinking global, acting European".[31] Where resilience-building and focus on the internal market remain dominant, matching

---

[23] Agnes Kasper, "EU Cybersecurity Governance – Stakeholders and Normative Intentions Towards Integration," in *The Future of the European Union: Demisting the Debate*, eds. Mark Harwood, Stefano Moncada, and Roderick Pace (Msida: Institute for European Studies, 2020), 169-170 (166-185).

[24] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (JOIN (2013), 1 final, Brussels, 2013).

[25] European Commission, 2017.

[26] Council, "EU Cyber Defence Policy Framework" (15585/14, Brussels, 2014).

[27] Council, 2018d.

[28] Council, "Non-Paper: Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations" (5797/2/16, Brussels, 2016).

[29] Council, "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Tool-box') – Adoption" (9916/17, Brussels, 2017).

[30] European Commission, 2020j.

[31] European Commission, 2020j.

the very character of the EU, its initiatives on operational capacity building at the EU level and hands-on international engagement substantially increased both in quantity as well as depth in comparison with the previous strategic document.

The above overview demonstrates the growing concern for economic, socio-political, diplomatic, and military aspects of cybersecurity at the EU level, and that the entity has a comprehensive approach to cybersecurity policy, encompassing areas from electronic communications through electronic signatures and trust services, to the fight against cybercrime and R&D in cyber defence.[32] Cybersecurity is a diverse policy area, which falls under the more general digital and global strategy frameworks of the EU, hence presumptively aspires for normative appeals. Intriguingly, the EU understands the context, evidently influencing third countries in how they should design their digital and cyber policies, or, as in the particular case of the "General Data Protection Regulation" (GDPR), simply designing a major policy for the rest of the world to use. Therefore, the question can be raised as to how this policy is supported in terms of narrating the EU's cyber power(s). The EU has consciously defined its contribution to global cybersecurity, and discussions in the Council took place in 2019 about the narrative in preparation to the then upcoming talks in the UN on cyber issues in the context of international security, suggesting the EU to focus on communication efforts to a) prevent conflicts; b) promote cooperation and c) build stability in cyberspace.[33] However, it is evident that there is more analytical depth in both the EU's cyber powers and a range of narrative, associated with these particular powers, than the Council managed to outline it. The following sub-chapter attempts to clarify the picture, in structural terms at least.

3. *Cyber power as a measurable phenomenon*

In order to shape the global cybersecurity landscape, the EU has to be relying on its strengths or powers, while projecting these in the process of cooperation with different non-EU others. The entity's

[32] Agnes Kasper and Alexander Antonov, "Towards Conceptualizing EU Cybersecurity Law," *ZEI Discussion Paper C 253/2019* (Bonn: Center for European Integration Studies, Universität Bonn, 2019), this and following links accessed 30 March 2021 [https://www.zei.uni-bonn.de/dateien/discussion-paper/DP-C253-Kasper_Antonov.pdf].

[33] European External Action Service, "Narrative Paper on an Open, Free, Stable and Secure Cyberspace in the Context of International Security" (9764/1 (2019), rev.1 of 5, Brussels, 2019a).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

achievements in the field of political economy —arguably, the most solid foundation for initiating and leading any kind of global change— can hardly be disputed. Jean-Claude Juncker, for example, portrayed the EU as "a trade power" and "the world's biggest single market" that "has trade agreements with 70 countries around the world, covering 40% of the world's GDP" and "accounting for a fifth of the world's economy".[34] Cyber power, however, is different from any other, and its dimensions are more about a tightly interlinked system of already existing capabilities. While several approaches to explaining and, to an extent, measuring the concept of cyber power in general, and the cyber power of Europe[35] in particular, are known, this research adopts Klimburg's Integrated Capability Model, while still recognising the value in other (possible) approaches.

The Model construes cyber power in terms of integrated capabilities – that of government, system and national levels.[36] In this view, capabilities refer to abilities, which manifest in some action, and a political entity has cyber power if it has the ability to shape aspects of the global cybersecurity landscape. These actions are visible in and are accompanied by communicative acts, which, when necessary, can also mean cooperative activities (*Table 1*). Characteristically for this contribution's discussional framework, the dimensions of cyber power outlined in the Model and fully supported by the EU's global outreach also align with the three types (or levels) of strategic narrative to be touched upon in the following part of this article. When discussing the findings, this analytical point leads us toward establishing an issue-specific schema where the cyber power-associated dimensions are interlinked with the Strategic Narrative Theory's instrumentarium, having cybersecurity-focused strategic communication as a base.

[34] Jean-Claude Juncker, "State of the Union 2018. The Hour of European Sovereignty," *The European Commission*, 2018, [https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_ en_0.pdf].

[35] Myriam Dunn Cavelty, "Europe's Cyber-Power," *European Politics and Society* 19, no.3 (2018), 304-320.

[36] Klimburg.

Table 1

European cyber power in the framework of the Integrated Capability Model

Dimension of Power	Ability to	Examples
Integrated government capability	— Deliver joint action — Attack and defend in cyberspace — Draft policy positions — Share operational resources	— ENISA/EU Cybersecurity Agency — EC3 (European Cybercrime Centre) — NIS (Network and Information System) Cooperation Group — 5G cybersecurity toolbox — Blueprint for cyber crisis management — Cyber-defence capabilities — CERT/CSIRT network — Cyber exercises — NIS strategies — Police Directive — 4Party MoU (EDA, EC3, EU-CERT, ENISA) — ESDC cyber courses
Integrated system capability	Work through international alliances and partnerships	— Cyber Diplomacy Toolbox — Bilateral cyber dialogues and agreements — External cyber capacity building — Involvement of the EU in international *fora* — Cooperation with NATO, UN, CoE, OSCE — Horizontal cooperation with non-state and hybrid organisations (FIRST, ICANN)
Integrated national capability	Use non-state cyber elements in direct support of policy (work together with infrastructure operators, software and hardware manufacturers, hackers, researchers, activists)	— EP3R (European Public-Private Partnership for Resilience) — R&D programmes — Cybersecurity standardisation and certification (Cybersecurity Act) — NIS framework — GDPR — European Cybersecurity Network and Competence Centre — Cyber hygiene and awareness raising

Source: adapted by authors from Klimburg and Dunn Cavelty.

As for the EU's cyber power in itself, it is seemingly not based on coercion, but rather on the idea of cooperation, collaboration and persuasion for taking part in the cyber-game (Dunn Cavelty). Thus, examining the manifestations, examples, context and "stories" relating to these elements of

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

cyber power can potentially lead toward detecting an EU (or even European) narrative about cyber power. For that, especially when it comes to a credible scheme that directly requires an integrated approach with regards to communication/cooperation (with NATO, OSCE, or ASEAN, for example), the EU's real, perceived and prospective power will, by necessity, be in need of being genuinely endorsed by a more unified EU with a sounder issue-specific strategic narrative.

II. **Crafting a discussion framework**

This research has an ever-increasing range of moderators, which effectively simplifies the process of data-gathering. For example, in June 2020, Commission President Ursula von der Leyen openly called out China for "targeting EU hospitals and health care institutions with cyberattacks during the coronavirus crisis".[37] A few days prior, the importance of the Asia-Pacific dimension within the global debate on cybersecurity was reinforced by Australian Prime Minister Scott Morrison who noted that a number of Australian organisations (both governments and businesses) were targeted by a sophisticated foreign "state-based" hacker, and that "there are not a large number of state-based actors that can engage in this type of activity".[38] Initially, discourse wise, the Australian side used the "You-Know-Who" diplomatic construct for a message formation, but, considering the worsening state of Australia-China interactions, a myriad of China-focused topics immediately made headlines in Australian media. On the local level of the EU, Estonian President Kersti Kaljulaid, keeping in mind that her country was the first that had to face a cyber-war, argued that "states are responsible for their activities in cyber-space [...] [and] their internationally wrongful cyber operations just as they would be responsible for any other activity based on international treaties or customary international law".[39]

---

[37] Ursula von der Leyen, "Von der Leyen Calls Out China for Hitting Hospitals with Cyberattacks," *Politico*, 2020b, [https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/eu-calls-out-china-for-hitting-hospitals-with-cyberattacks/amp/].

[38] Scott Morrison, quoted in Georgia Hitch and Andrew Probyn, "China Believed to be Behind Major Cyber Attack on Australian Governments and Businesses," *ABC News*, 2020, [https://www.abc.net.au/news/2020-06-19/foreign-cyber-hack-targets-australian-government-and-business/12372470].

[39] Kersti Kaljulaid, "President of the Republic at the Opening of CyCon 2019," *Office of the President*, 2019, [https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/].

Considering the above, the process of data gathering for this article is a reasonably straight-forward exercise, being methodologically operated by the rules of meticulous normative discourse analysis and process tracing. The main variables of this research —the EU's strategic plans and actions on cybersecurity and the current level of the entity's direct involvement in international cooperation on the issue— allow for enhancing all types of epistemological platforms. The material's discussion framework, however, is an academic *nouveauté*, which features a significant degree of multifacetedness. In general, it makes use of the postulates of Strategic Narrative Theory that, principally, does not go against an easily justifiable assumption that the EU has some capabilities to influence a range of core aspects of the global cybersecurity landscape, while solidifying its own identity, system, and policy narratives. Thus, the analytical "twist" here is about interlinking the popular theory concretely with the EU's cyber power(s), rather than rehashing the discussion of the entity's "soft power" (from where the Strategic Narrative Theory materialised into being one day). After all, as noted, cyber power is measurable, and this feature of the phenomenon adds practicality to the whole discussion. A good degree of measurability could also be considered a definite methodological bonus to the process of observing how the EU formulates and projects its strategic narratives to ensure their welcome reception elsewhere. At the same time, a polemic on a cyber power Europe that "manufactures" plenty of strategic narratives evidently does not bring a student of international relations closer to what the EU really is and how it communicates with the world. A *secret académique de Polichinelle* about the EU's imperial nature and the entity's participation in the process of redesigning the international system are of definite help on this occasion though.

1. *Communication as a power resource of a non-conventional empire*

As it was noted before, the EU is not alone in trying to make a substantial difference in the field. These days, arguably, the focus of key agents and entities is on re-development of the international system. Indeed, the EU, has long been discussed and depicted as a normative power,[40] whatever it might mean, and its political (but almost never geo-strategic) ethos of conflict prevention, reconciliation, collective action and sustainable peace has informed the entity's external action throughout its existence. The point being that the "base" for the post-World War II (WWII) international system,

[40] Ian Manners, "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 40, no.2 (2002), 235-258.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

became an archaic element of the difficult past, let alone the then convenient concept of the "world's five policemen".[41] Arguably, the geo-strategic spirit of Yalta belongs to history – even at first glance, the Russian Federation is no match to the former Soviet Union in almost all possible respects, Chiang Kai-shek and Mao Zedong are in no ideological competition any more, both France and Britain are by far no super-powers, and global interrelations are featured by the existence of powerful actors like the EU, NATO, OPEC, or ASEAN, which would never be visualised to exist in 1945.[42]

In this context, Bisley, predicting the nature of a problem that the UN-bound international order would be facing, argued that "the assumptions of great power managerialism" was "severely challenged by contemporary circumstances".[43] Therefore, openly or latently, China, the EU, Russian Federation, and the USA are working "overtime" to revitalise the good old imperial paradigm, perhaps trying to re-frame the Lacanian "social bond" they have always had with their peripheries (often meaning the rest of the world) and erasing the imperial paradigm from the dialectic of perceived negativity, all for the visible enjoyment of students of international relations. Indeed, there is a sizable segment of current academic research — Howe,[44] Terrill,[45] Zielonka,[46] Motyl,[47] Parker,[48] Gravier,[49] Dimitrovova,[50]

---

[41] Serhii Plokhy, *Yalta: The Price for Peace* (New York: Viking Penguin, 2010).

[42] Vlad Vernygora, "A Place for Ukraine in a More Cohesive European Union: Synergising the Two Different Integrations," eds. Liubov Akulenko and Dmytro Naumenko (Ukrainian Centre for European Policy, 2019), 20, [https://ukraine-office.eu/en/a-place-for-ukraine-in-a-more-cohesive-european-union-synergising-the-two-different-integrations/].

[43] Nick Bisley, *Great Powers in the Changing International Order* (Lynne Rienner Publishers, 2012), 182.

[44] Stephen Howe, *Empire: A Very Short Introduction* (Oxford: Oxford University Press, 2002).

[45] Ross Terrill, *The New Chinese Empire* (Sydney: UNSW Press, 2003).

[46] Zielonka, 2006; Jan Zielonka, "America and Europe: Two Contrasting or Parallel Empires?" *Journal of Political Power* 4, no.3 (2011), 337-354; Jan Zielonka, "Empires and the Modern International System," *Geopolitics* 17, no.3 (2012), 502-525; Jan Zielonka, "The International System in Europe: Westphalian Anarchy or Medieval Chaos?" *Journal of European Integration* 35, no.1 (2013), 1-18.

[47] Alexander J. Motyl, "Thinking about Empire," in *After Empire: Multiethnic Societies and Nation Building*, eds. Karen Barkley and Mark von Hagen (Oxford: Westview Press, 1997), 19-29; Alexander J. Motyl, *Revolutions, Nations, Empires: Conceptual Limits and Theoretical Possibilities* (New York: Columbia University Press, 1999); Alexander J. Motyl, *Imperial Ends: The Decay, Collapse, and Revival of Empires* (New York: Columbia University Press, 2001).

[48] Parker, 2008; Noel Parker, "Empire as a Geopolitical Figure," *Geopolitics* 15, no.1 (2010), 109-132.

[49] Gravier.

[50] Bohdana Dimitrovova, "Imperial Re-bordering of Europe: The Case of the European Neighbourhood Policy," *Cambridge Review of International Affairs* 25, no.2 (2012), 249-267.

Vernygora,[51] Vernygora *et al*.,[52] and others— that observes contemporary empires and detects a particular degree of peculiarity in the relationships between an empire's centre and its periphery, which on an increasingly high number of occasions represents the rest of the globe.

In order to adequately respond to a number of diverse challenges, an empire has to practice different types of strategic communication with the world. In imperial terms, "communication", by necessity, means "cooperation" or, in some cases, "enforcement of cooperation" —but the scheme of/for actions needs to be formulated each time.[53] Evidently, an imperial "conversation" that Russia is having with Ukraine can be classified as a hybrid war.[54] However, when China strategically designates a European region to cooperate with (the so-called 16+1, if Lithuania is not counted, framework as an integral part of the Belt and Road Initiative/BRI), it can relate to a different type of cooperation— more associated with ruthless functionalism, socio-political construct building and some neo-functional tendencies.[55] For the European continent, of course, the latest Chinese imperial "march" adds plenty of neoteric peculiarities into the EU-centric process of *intra-* continental European integration, but, as suggested, it also motivates "the EU to think more strategically",[56] and arguably compliments the fact that "Beijing has become an indispensable actor in the post-Soviet space"[57]

---

[51] Vlad Vernygora, "The Unbearable Lightness of Permanent Integration: Why Does the EU Need to Answer its Ukrainian Question?" *The Australian and New Zealand Journal of European Studies* 5, no. 2 (2013), 92-94; Vlad Vernygora, "The Belt and Road: Gently Rebuffing Geo-Politics?" in *China-CEEC Cooperation and the "Belt and Road Initiative"*, eds. Ping Huang and Liu Zuokui (China Social Sciences Press, 2016), 1-12.

[52] Vlad Vernygora, David Ramiro Troitiño, and Sigrid Västra, "The Eastern Partnership Programme: Is Pragmatic Regional Functionalism Working for a Contemporary Political Empire?" in *Political and Legal Perspectives of the EU Eastern Partnership Policy*, eds. Tanel Kerikmäe and Archil Chochia (Springer International Publishing, 2016), 7-22.

[53] Vlad Vernygora and Elizaveta Belonosova, "A Modern Empire and Its Public Diplomacy: On Russia's Communication with Estonia," a Special issue of *New Zealand Slavonic Journal* 53-54 (2019-2020), 59-93, eds. Natalia Chaban, Henrietta Mondry, and Evgeny Pavlov. Published in 2021..

[54] Gjorgji Veljovski, Nenad Taneski, and Metodija Dojchinovski, "The Danger of 'Hybrid Warfare' From a Sophisticated Adversary: the Russian 'Hybridity' in the Ukrainian Conflict," *Defense & Security Analysis* 33, no.4 (2017), 292-307.

[55] Vernygora, 2017.

[56] Andris Sprūds, "Towards a Balanced Synergy of Visions and Interests: Latvia's Perspectives in 16+1 and Belt and Road Initiatives," a Special issue of *Croatian International Relations Review* 23, no. 78 (Zagreb: Institute for Development and International Relations, 2017), 50 (37-56), eds. Senada Šelo Šabić and Vlad Vernygora.

[57] Konstantinas Andrijauskas, "The Grand Strategic Nature of China's Current International Infrastructure-related Projects," in *China-CEEC Cooperation and the "Belt and Road Initiative"*, eds. Ping Huang and Liu Zuokui (China Social Sciences Press, 2016), 36 (27-38).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

regardless of what Russia, the EU, and the United States might be thinking of it.

Back to the theme, the EU's initial introverted vision on cybersecurity turned into a comprehensive "conversation", focusing on both internal and external aspects such as cyber resilience, capacity building and strategic autonomy. The latter concept came from one of the biggest geo-strategic debacles in the EU's history —"A Global Strategy for the European Union's Foreign and Security Policy"[58]— that unsuccessfully attempted to deliver the EU's strategic "message" when the United Kingdom EU membership referendum's results had just been announced. However, the 2017 and 2020 Cybersecurity Strategies managed to "get back on track" and underline a few points on strengthening international cooperation and creating effective cyber deterrence. Moreover, a high-level panel at The Riga Conference,[59] working under the Chatham House Rule, seriously discussed the conceptual vagueness of the EU's strategic autonomy. A legitimate question was asked then on whether or not the EU should become more strategically responsible rather than autonomous. Another side of the same question was related to the possible outreach —how far, geographically or in any other understanding, can or should the EU go in terms of communicating in strategic terms? For example, the Russian Federation, the EU's geo-strategic "competitor", has already made its call on geography when the country's President Vladimir Putin suggested that Russia's border "doesn't end anywhere".[60] The cyber world, naturally, also does not comprehend geography— in this sense and on this occasion, Hardt and Negri with their "there is no more outside"[61] are objectively spot on. Thus, there is a likelihood that, with its more articulated as well as internationally recognised stance on cybersecurity, the EU can avoid becoming geo-strategically irrelevant.[62] This is where, methodologically, a strategic message of a cyber power, in order to be effective, requires quite a process to go through-to be formulated, projected, and then positively received.[63]

---

[58] European External Action Service, 2016.

[59] The Riga Conference, "Night Owl Session: EU Strategic Autonomy vs. EU Strategic Responsibility?" (Riga, 11 October 2019).

[60] Vladimir Putin, quoted in "Russia's Border Doesn't End Anywhere, Vladimir Putin Says," *BBC*, 2016. [https://www.bbc.com/news/ world-europe-38093468].

[61] Hardt and Negri, 186-190.

[62] Kasper and Vernygora, 204.

[63] Roselle *et al*., 78-79.

2. *Strategic narratives: a 'salad' made out of soft power, discourses, and practicality*

"In the beginning was the […]"[64] concept of "soft power". Having coined it, Nye produced a compelling double-sided narrative on the concept, indirectly giving jobs to thousands of political scientists and directly arguing that a) "[t]he United States cannot obtain the outcomes it wants on trade, antitrust, or financial regulation issues without the agreement of the European Union, Japan, China, and others" and b) "[a] country may obtain the outcomes it wants in world politics because other countries admiring its values, emulating its example, aspiring to its level of prosperity and openness want to follow it".[65] A few years later, the same author offered a seminal elaboration on how soft power is (or can be) interlinked with "public diplomacy",[66] and the analytical "ball" on the issue started rolling. Indirectly, this work was expended upon by Zielonka who elegantly discussed "the role of pride, glory, morality or religious zeal" in the field of international relations, while arguing that the "export of 'good' governance"[67] represents the essence of the EU's imperial civilising mission. However, Roselle *et al*. did the rest, having suggested that it would still be hard to "(1) identify soft power resources, (2) identify the processes through which soft power operates, and (3) understand under what conditions soft power resources can be used to support foreign policy".[68] Their argument was that, in a "chaotic world", a substantial assistance in making sense of soft power should be arriving from the communicational side; more specifically, from our understanding of "a compelling narrative" as "a power resource", since "people may be drawn to certain actors, events, and explanations that describe the […] specifics of a policy".[69]

Having extrapolated Burke's[70] major study into the field of international relations, Roselle *et al*. offered the following classification of component parts of narratives, namely "character or actors", "setting/ environment/space", "conflict or action", and "resolution or suggested resolution", underlining the point that "a narrative about the international

---

[64] A part of the initial line from *The Gospel of John*.

[65] Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), 4-5.

[66] Joseph Nye, "Public Diplomacy and Soft Power," *The ANNALS of the American Academy of Political and Social Science* 616, no.1 (2008), 10-30.

[67] Zielonka, 2012, 504 and 511.

[68] Roselle *et al*., 74.

[69] Roselle *et al*., 74.

[70] Kenneth Burke, *Language as Symbolic Action: Essays on Life, Literature, and Method* (Los Angeles: University of California Press, 1966).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

system that stresses the importance of international cooperation to confront those who break norms about [for example] chemical weapons, highlights 'acceptable' behavio[*u*]r in the international system".[71] For the theme of this research, such a classification is a great "gift" that assists in the process of placing the right element of a narrative's cycle into the right analytical "basket" where component parts of the same type are already placed. Arguably, it is good news for an entity (the EU?) that would be ever on a quest to strategically narrate its cyber power —the actors are already in the first row watching the unlimited space of the cyber domain, while getting engaged in numerous conflicts and working on (or awaiting for) a solution on how to walk the walk in cyber world. The theory's practical applicability in terms of framing up and/or analysing a co-operational platform was, however, more precisely outlined by Miskimmon *et al*. in a larger volume where strategic narratives were presented at three different levels— national (or identity), system, and issue (or policy).[72] In a way, the idea existing behind the scheme is nearly self-explanatory, but, as already noted, this classification is useful for this article in the process of interlinking it with the dimensions of cyber power.

It deserves to be mentioned that the theory has been extensively "employed" in the process of analysing the images of NATO as a cooperative security actor in media and elite discourses of Australia, Japan, Mongolia, New Zealand, and the Republic of Korea.[73] The body of serious literature applying Strategic Narrative Theory to the EU grows as well. For example, a study on "broader narratives of the EU as a diplomatic and security actor, in conflicted societies"[74] made a significant contribution to perceptions studies in the EU's designated immediate neighbourhood. Kurowska's research on the highly contested politics of cyber norms made the point that the EU's "cyber diplomacy" could, in principle, engage in "strategic narrative contestation in order to shape the process of Internet governance more meaningfully and contemporaneously".[75] Therefore, the

---

[71] Roselle *et al*., 75-76.

[72] Miskimmon *et al*.

[73] Chaban, Natalia, Paul Bacon, Joe Burton, and Vlad Vernygora, "NATO Global Perceptions – Views from the Asia-Pacific Region," a Special issue of *Asian Security* 14, no. 1 (Taylor and Francis, 2018), eds. Natalia Chaban, Paul Bacon, Joe Burton, and Vlad Vernygora.

[74] Chaban, Natalia, Alister Miskimmon, and Ben O'Loughlin, "Understanding EU Crisis Diplomacy in the European Neighbourhood: Strategic Narratives and Perceptions of the EU in Ukraine, Israel and Palestine," a Special issue of *European Security* 28, no. 3 (2019), 235 (235-250), eds. Natalia Chaban, Alister Miskimmon, and Ben O'Loughlin.

[75] Xymena Kurowska, "The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation," *EU Cyber Direct* (2019), [https://eucyberdirect.eu/wp-content/uploads/2019/05/xymena-kurowska-politics-of-cyber-norms-march-2019-eucyberdirect.pdf].

theory-associated instrumentarium can arguably be considered "durable" enough to frame a solid platform for discussion on the EU's prospective leading role in the process of shaping the global cybersecurity environment.

IV. **EU cyber (power) narratives**

With the basic terminological postulates outlined, it is time to put the grand empirical picture together and identify different narratives the EU may have formulated (or be in the process of formulating) about its cyber power (its integrated government, system and national cyber capabilities). First, this article's focus is internal, however the EU's *intra*-world is undeniably interlinked with external issues. Cybersecurity-associated concerns became noticeable on the EU-level by the mid-1990s, remaining concentrated on the idea of the European Single Market for a long period. Personal data protection and data security were the first to make it to EU level politics and resulted in the 1995 Personal Data Protection Directive where security enjoyed some limited attention.[76] Under the first pillar of the EU, created by the Maastricht Treaty, telecommunication sector regulation necessitated consideration of security. In 1994, a set of high-end recommendations to the European Council —the Bangemann Report on "Europe and the Global Information Society"— pointed out the importance of encryption in the context of e-commerce and personal data protection, suggested the need for international standards, and urged the creation of an appropriate legal framework. The material argued that, due to the cross-border nature of cyberspace, "a solution at the European level is needed which provides a global answer to the protection of encrypted signals and security".[77]

In 1994, the Corfu-hosted Summit of the European Council took a note on the Bangemann Report and addressed the challenges of the information society in its Presidency Conclusions, stating that "it is primarily for the private sector to respond to this challenge".[78] At the same time, the European Council also considered that "the importance and complexity of

[76] European Parliament and the Council, "Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (95/46/EC, Strasbourg, 1995), Art. 17.

[77] "Europe and the Global Information Society —Recommendations to the European Council, Conference G7— Raport Bangemann" (Luxembourg: Office for Official Publications of the European Communities, 1994), 22-23, [https://op.europa.eu/en/publication-detail/-/publication/44dad16a-937d-4cb3-be07-0022197d9459/language-en].

[78] European Council, "Presidency Conclusions," (6/94, Corfu, 1994).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

the issues raised by the new information society justify the setting up of a permanent co-ordination instrument to ensure that the various parties involved —public and private— are working along the same lines", and committed to Community level action stating that "the necessary regulatory framework has to be established as soon as possible".[79] These first steps in the field of cybersecurity[80] defined the overall attitude of the EU on the issue for years to come: a permanent coordination instrument was conceived, from which the integrated government cyber capability could emerge; the initiative emphasised the role of the private sector, which can be used as a basis to integrate national cyber capabilities to support potential EU-level policies on the theme. Even so, it was clear that the policy remained internally focused, and integrated system cyber capabilities would likely be working indirectly through economic policy.

In 1999, the Tampere-hosted Summit addressed the need for an EU-wide fight against criminal activity and underscored the body's commitment "to reinforcing the fight against serious organised and transnational crime",[81] making a specific reference to high tech crime. Indeed, cybersecurity started entering international relations in the end of 1990s (in particular, with the Russian Federation's proposal for a convention on information security at the UN). However, the EU's structure and competences did not make it possible to make a significant impact and meaningfully engage with international actors as a single entity, even though, under the second pillar, the EU became active in the fight against cybercrime. The 2001 Commission Communication "Network and Information Security: Proposal for A European Policy Approach" clarified how the EU viewed the structure of the problem, having noted that "[s]ecurity is be-coming a key priority because communication and information have be-come a key factor in economic and societal development".[82] Hence, the EU made another step beyond the well-functioning Single Market, recognising for the first time that three policy areas —network and information security, cybercrime, and data protection/ telecom framework— are closely interrelated. In retrospect, this document is worth noting for presenting network and information security as a national security concern because, as stated, "information systems and communication networks have become a critical factor for other infrastructures (e.g. water

[79] European Council, 1994.

[80] It should be noted that the notion of "cybersecurity" was not used in early policy documents, and its terminological usage remains somewhat inconsistent to date.

[81] European Council, "Presidency Conclusions" (Tampere, 1999), [https://www.europarl.europa.eu/summits/tam_en.htm].

[82] European Commission, "Network and Information Security: Proposal for a European Policy Approach" (COM (2001), 298 final, Brussels, 2001).

and electricity supply) and other markets (e.g. the global finance market)".[83] While the material's analysis, from a vertical perspective, mainly depicted non-governmental actors and their roles in cyberspace, it also mentioned horizontal issues such as a certain level of dependence on the USA's export control policy, as well as the ECHELON scandal and potential damage to public sector and industry.[84] Via this document, the Commission proposed a comprehensive policy, where the external dimension became an integral element of assessment, and international cooperation – an indispensable part of narratives about cybersecurity.

However, it took years for this ambitious approach of the Commission to gain traction, and the proposal for measures that correspond to the integrated system capability remained modest. It merely stated that the Commission would "reinforce the [ongoing] dialogue with international organisations and partners on network and information security",[85] and seemingly relied on the spontaneous engagement of the private sector in international *fora*. A palpable deliverable in integrated government cyber capabilities was the establishment of the European Network and Information Security Agency (ENISA) in 2004, which was tasked to "assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the internal market".[86] The Agency's objective was to "enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems",[87] however this would be achieved via providing assistance and delivering advice, developing high levels of expertise and stimulating cooperation between public and private actors.[88]

A significant shift in the EU's view about the international order in the cyber domain was also set in motion after 9/11. The 2003 European Security Strategy, "A secure Europe in a better world", made a reference to an emerging cyber threat, although within the context of discussing the conventional security threat of terrorism, and stated that "[i]ncreasingly, terrorist movements are well-resourced, connected by electronic networks,

[83] European Commission, 2001.
[84] European Commission, 2001, 11-12.
[85] European Commission, 2001, 27.
[86] European Parliament and the Council, "Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency" ((EC) 460/2004, Strasbourg, 2004), Art. 1(2).
[87] European Parliament and the Council, 2004, Art. 2(1).
[88] European Parliament and the Council, 2004, Art. 2(2-3).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

and are willing to use unlimited violence to cause massive casualties".[89] In 2006, a further push from the European Commission in the form of a Communication on "A strategy for a secure information society – Dialogue, partnership and empowerment" emphasised the importance of research and development through the Sixth and Seventh Framework Programmes and related projects[90], as well as the active role of the EU in international fora addressing these topics.[91] Then the European Commission recognised that a breach in network and information security "can generate an impact that transcends the economic dimension", and in this context it pointed out that security is a prerequisite for guaranteeing fundamental rights online and that linked critical infrastructures are at risk due to their dependence on information and communication technologies.[92]

A clear turning point in the framing of cybersecurity came when Javier Solana reported on the implementation of the European Security Strategy and concluded that "[cyber]attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon".[93] This was not, however, an invention of the EU as, following the two-month long cyber attack against Estonia in 2007, cybersecurity had become a mainstream topic in international relations.[94] As a direct reflection of the cyber war, in May 2008, the NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn.[95]

Arguably, the EU's understanding of cybersecurity has incrementally developed from a narrow sectoral issue into a comprehensive view. Although the actorness of the EU and the coherence of its policy still remain as debated topics,[96] the changes introduced by the Lisbon Treaty

---

[89] Council, "European Security Strategy. A Secure Europe in a Better World" (15895/03, Brussels, 2003), 30.

[90] Including integrating national cyber capabilities and engaging the non-governmental sector in responding to cyber threats, etc.

[91] European Commission, "A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment" (COM (2006), 251 final, Brussels, 2006).

[92] European Commission, 2006.

[93] Javier Solana, "Report on the Implementation of the European Security Strategy – Providing Security in a Changing World," *European Communities*, 2009, [https://www.consilium.europa.eu/media/308 23/qc7809568enc.pdf].

[94] Liis Vihul, "International Law of Cyber Defence," in *Handbook of Cybersecurity*, ed. Jochen Rehrl (Federal Ministry of Defence of the Republic of Austria, 2018), 28 (27-34).

[95] NATO Cooperative Cyber Defence Centre of Excellence, "The NATO Cooperative Cyber Defence Centre of Excellence is a Multinational and Interdisciplinary Cyber Defence Hub" (Tallinn, 2020), [https://ccdcoe.org/].

[96] Helena Carrapiço and Andre Barrinha, "The EU as a Coherent (Cyber)security Actor?" *Journal of Common Market Studies* 55, no.6 (2017), 1254- 1272.

created a geo-strategic climate, from where the process of moving forward with an ambitious cybersecurity policy became possible. The following years have been referred to as a "cyber awakening",[97] and references to internationally significant cyber incidents started featuring in various communications by the EU and the entity's leadership. In a 2009 press-release on the Transport, Telecommunication and Energy Council meeting, the then "[r]ecent events such as the cyber-attacks against Estonia in 2007 and the fractures in transcontinental cables in 2008" were referred to and used to "show the vulnerability of modern information networks and underline the importance of protective measures aimed at ensuring continuation of critical services".[98]

The EU intensively focused on combating cybercrime, leading to the adoption of the "Botnet Directive"[99] and the creation of the European Cybercrime Centre (EC3) to support Member States and EU institutions in building an operational as well as analytical capacity for investigations and cooperation with international partners.[100] In addition, several other documents addressed cybersecurity and critical information infrastructure protection in tandem, such as the Commission Communication on "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience",[101] and the Council Conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP)'.[102] Finally, in November 2012, the EU's Foreign Affairs Council welcomed pooling and sharing projects supported by the European Defence Agency, including areas of Cyber Defence, and raised the cyber issue again in the context of defence industry and market.[103] By 2013, cybersecurity became a strategic issue to include all

---

[97] Heli Tiirmaa-Klaar, "Two Generations of EU Cybersecurity Strategies," in *Handbook of Cybersecurity*, ed. Jochen Rehrl (Federal Ministry of Defence of the Republic of Austria, 2018), 18 (18-26).

[98] Council, "2949th Council Meeting, Transport, Telecommunications and Energy" (10850/09 (Presse 169), Luxembourg, 2009).

[99] European Parliament and the Council, "Directive of the European Parliament and of the Council on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA" (2013/40/EU, Strasbourg, 2013).

[100] Council, "Draft Council Conclusions on the Establishment of a European Cybercrime Centre" (10603/12, Brussels, 2012a).

[101] European Commission, "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience" (COM (2009), 149 final, Brussels, 2009).

[102] Council, "Critical Information Infrastructure Protection 'Achievements and Next Steps: Towards Global Cyber-security' (CIIP)" (10299/11, Brussels, 2011).

[103] Council, "3199th Council Meeting Foreign Affairs" (16062/12 (Presse 467), Brussels, 2012b), [https://ec.europa.eu/commission/presscorner/detail/en/PRES_12_467].

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

EU major competence areas, viewed as a whole-of-government approach as formulated in the 2013 Cybersecurity Strategy.[104]

On a concrete note of a particular strategic narrative's formulation, the 2013 Cybersecurity Strategy evidently depicted a new global environment that has emerged gradually and influences most aspects of everyday life. Arguably, economies, social interactions, exercise of fundamental rights depend on the seamless functioning of the underlying information and communication technologies, where malicious activities, misuse and accidents are considered as major threats to economic growth, safety and respect of fundamental rights online. The document did not make a clear distinction between the origin of these threats, thereby acknowledging that the boundaries between external and internal policies were increasingly blurred in cyberspace. However, it specified a range of threat agents to go after: cybercriminals, state actors engaging (sponsoring) in controversial cyber operations and governments misusing cyberspace for surveillance and exerting control over their citizens. The EU identified itself as the guardian of the highest possible freedom and security for the benefit of all, and it lay out five priorities to this end, all of which formed the subject of discourse previously in one way or another. Nevertheless, in 2013, they were formulated under one policy umbrella and extended more broadly, stretching the EU's competences further into increasingly sensitive policy domains. These priorities included the focus on network and information security, framed as achieving cyber resilience; reducing cybercrime; developing cyber defence policy and related capabilities; developing the industrial and technological resources for cybersecurity; and establishing a coherent international cyberspace policy for the EU and promoting core EU values.[105]

Since the global cyber-threat environment evolved in 2016-2017, the EU's strategic stance on the issue has also been upgraded and formulated in the "Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU".[106] The focus of the strategy somewhat shifted from the predominantly economic focus to emphasise that cyberspace is a source of serious political and military threats, capable of jeopardising "the very functioning of our democracies, our freedoms and our values".[107] Hence cyber threats "come from both non-state and state actors: they are often criminal, motivated by profit, but they can also be political and strategic" and "state actors are increasingly meeting their geopolitical goals not only through

[104] European Commission, 2013.
[105] European Commission, 2013.
[106] European Commission, 2017.
[107] European Commission, 2017.

traditional tools like military force, but also through more discreet cyber tools, including interfering in internal democratic processes".[108] While referring to recognisable international cyber incidents (ransomware campaigns,[109] cyber operations against critical infrastructure,[110] disinformation campaigns, *et cetera*), and pointing out that the economic impact of cybercrime increased fivefold in the period from 2013 to 2017, the EU started formulating and projecting a single important message about the cyber environment: the existing system is increasingly unpredictable at all levels.

Integrated government capabilities have been at the core of the EU's approach, for which ENISA was established and since transformed into a more powerful Cybersecurity Agency by the 2019 Cybersecurity Act.[111] Although ENISA's new powers and competence come with limitations, it represents the cornerstone of the integrated government capability, together with the NIS Directive.[112] ENISA/Cybersecurity Agency also has some tasks in the field of international relations and defence. Therefore, this institutional setup implies that in the new cyber order the internal and external issues are commingled, nevertheless enabling more joint action on the level of governments. ENISA/ Cybersecurity Agency embodies the generation of cyber power in both tackling diverse cyber-related issues (sectoral and horizontal), aims to engage national level and private actors in the policy processes, and liaises between actors and sectors (for example concluded an agreement with Europol and EDA, exhibiting its integrated national cyber capabilities). However, this is not yet the ultimate solution, since the strategies and the architecture of the legal framework still makes it clear that Member States are mainly responsible for cybersecurity, and the EU has a supporting, coordinating and advisory role, while the role of the private sector is also strongly emphasized.

While at the integrated system level the EU presents itself as a stabiliser, a civilising and pragmatic actor accepting value pluralism and seeking order and stability in cyberspace, the recent focus on the militarisation of cyberspace and its defence focus in the 2017 Cybersecurity Strategy managed to formulate a number of questions about the concept of strategic autonomy

---

[108] European Commission, 2017.

[109] The WannaCry, Petya and NotPetya malwares rampaged across the globe in 2017.

[110] Stuxnet, Black-Energy and other malwares disrupted critical infrastructures in preceding years.

[111] European Parliament and the Council, "Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act)" ((EU) 2019/881, Strasbourg, 2019).

[112] European Parliament and the Council, "Directive of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union" ((EU) 2016/1148, Strasbourg, 2016).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

and the role of the EU. The lack of clarity about its strategic autonomy or rather dual view of the future —a reminder of the story about Schrödinger's cat in the box— as well as the fact that true competence and deep expertise in cybersecurity resides outside the EU (at a national level in France, Germany and the Netherlands, for instance) is what lies behind the current modest role of the EU in 'hard' cyber defence.

It could be suggested that it occurs because the EU still does not mind "entertaining" the "inborn" intergovernmental nature of its Common Foreign and Security Policy (CFSP). Moreover, as argued, the status quo is being reinforced by France, the pre-COVID-19 EU's "front-runner in the process of establishing a new vision on a new Europe"[113] In May 2019, for example, *La République En Marche*, the political party of the French President Emmanuel Macron, published an important programming document, Projet Renaissance. The material had a range of proposals on major issues, namely "increased investment in environmental policy, imposing a tax on Big Tech across Europe, and moves toward a European army".[114] In terms of geo-strategy, *Projet Renaissance*, however, was very shy in formulating a prospective strategic narrative on the EU's more articulated global position in the international system. Speculatively, as suggested, "President Macron has a distinctly modest attitude towards making CFSP have a louder voice in global affairs [...] because France reserves this role … for France".[115] This is positive news for Yalta-1945 to "come back from the dead", but the EU is not to be found among decision-makers in that system.

It could be argued that via its current level of integrated system capability and ability to work through alliances, the EU relies on its normative and market powers to make a difference in how the international "cyber game" is played. The 2020 Cybersecurity Strategy is clear on the principal instruments deployed —regulation as well as investment and policy instruments,[116]— setting out a plan to engage in all kinds of international rule-setting, starting from international standardisation to responsible state behaviour in cyberspace, from international law's application in cyberspace to additional protocol to the Budapest Convention, not ignoring frameworks on protecting and promoting fundamental and human rights. More so, the document also reveals plenty on the EU's plan to form EU Cyber Diplomacy Network in order to promote the EU vision of cyberspace, exchange information, and regularly coordinate on developments in cyberspace.

---

[113] Vernygora, 2019, 21.

[114] Rym Momtaz, "Macron Unveils Plan for Europe," *Politico*, 2019, [https://www.politico.eu/article/macron-plan-europe-tech-renaissance/].

[115] Vernygora, 2019, 21.

[116] European Commission, 2020j.

The 2020 Cybersecurity Strategy can be regarded as a noticeable step forward in demonstrating the EU's growing cyber power to the global audience. Significant improvements in abilities to deliver a joint action or attack and defend in cyberspace, draft policy positions and share operational resources are planned based on existing practices. Some of the most tangible examples of such existing integrated government capabilities is the implementation of the cyber sanctions regime and imposition restrictive measures in the form of travel bans and asset freezes on more than one occasion;[117] the recent agreement on the establishment of the new Cybersecurity Competence Center and network aimed to pool expertise in cybersecurity across the EU;[118] or the decision to turn EMPACT (European Multidisciplinary Platform Against Criminal Threats) into a permanent tool to continue disrupting criminal activities related to attacks against information systems, particularly those following a crime-as-a-service business model and working as enablers for online crime.[119] The EU's plan to set up the Military CERT-Network may prove to be a particularly ambitious, but, if implemented, it should significantly increase the level of cooperation between the Member States and contribute to EU cyber power (perhaps, also with ability to attack in cyberspace) and the plan to develop an EU position on the application of international law in cyberspace (whereas until just recently most states were reluctant to publicly state their positions at all).

V. **The EU's external engagement in the field**

1. *Global cyber diplomacy of the EU*

The external dimension has been a core element of the EU's cybersecurity-related policies from the outset, although the actual competences of the EU, as discussed, has not always made it possible to actively engage in certain

[117] Council, "EU Imposes the First Ever Sanctions Against Cyber-Attacks" (Brussels, 2020a), [https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/]; Council, "Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body Over 2015 Bundestag Hack" (Brussels, 2020b), [https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/].

[118] Council, "New Cybersecurity Competence Centre and Network: Informal Agreement with the European Parliament" (Brussels, 2020c), [https://www.consilium.europa.eu/en/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/].

[119] Council, "Cybersecurity: How the EU Tackles Cyber Threats" (2021), [https://www.consilium.europa.eu/en/policies/cybersecurity/].

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

activities. The international link was emphasised in the context of critical information infrastructure (CII) protection in the 2009 Communication "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", stating that "[n]o country is an island… [and] the global nature of CII, and in particular of the Internet, requires a common global approach to security and resilience" and that "[i]t is via a strong EU coordination that a direct impact can be made at the international level".[120] In addition, the international level policy was also one of the five main points in the 2013 EU Cybersecurity Strategy where it explicitly formulated that its "cyberspace policy" is, in fact, "international", and that "the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyber-space".[121] The same strategic document also underlined that the EU will be working "towards closing the digital divide, and will [be] actively participat[ing] in international efforts to build cybersecurity capacity", while the entity's "international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights".[122] This can be considered a clear indication of the EU's global civilising mission and intention to formulate the issue-specific narrative internationally.

The external aspects of cybersecurity are also elaborated or referred to in several documents, general and specific where a predominantly *intra*-oriented view is presented in terms of cyber resilience, however adding that "the EU will enhance its cyber security cooperation with core partners such as the US and NATO".[123] In this context, it is worth mentioning that 21 Member States of the EU are NATO members as well, and many clusters of interactions between NATO and its partners across the globe (Afghanistan, Australia, Colombia, Iraq, Japan, the Republic of Korea, Mongolia, New Zealand, and Pakistan) include cooperation in the field of cybersecurity.[124]

In principle, significant developments have taken place since the original Global Strategy was published, and now the EU evidently possesses an important range of specific instruments dealing with cyber diplomacy,[125]

---

[120] European Commission, 2009.

[121] European Commission, 2013.

[122] European Commission, 2013.

[123] European External Action Service, 2016.

[124] NATO, "Relations with Partners Across the Globe" (Brussels, 2017 (last updated)), [https://www.nato.int/cps/en/natohq/topi cs_49188.htm]; Chaban *et al*., 2018.

[125] Council, "Council Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States" (7299/19, Brussels, 2019b).

industrial policy concerning the security of new technologies[126] *et cetera*. However, the Union has also exercised self-restraint in its external relations and in the context of its own guidelines.[127] While it has generally condemned the malicious use of information communications, including the WannaCry and NotPetya malware, it has not publicly attributed attacks (despite many countries having done so) until recently. Intriguingly, for a massively powerful entity with distinct imperial characteristics, the Council of the EU explained that "[i]t is not for the Council to comment on national governments' decisions, based on all-source intelligence, to publicly attribute cyber attacks to a state actor",[128] effectively admitting a significant gap in the EU's integrated system and government cyber capability. Condemnation of malicious cyber activities by the EU remained abstract, typically being worded such as in a declaration of Josep Borrell that the EU and its Member States "condemn [...] malicious behaviour in cyberspace", "[a]ll perpetrators must immediately refrain from conducting such irresponsible and destabilising actions", "call[ing] upon every country to exercise due diligence and take appropriate actions against actors con- ducting such activities from its territory".[129]

As a significant element of the EU's cybersecurity policy, capacity building is an important tool with internal and external effects – an effective means in the contemporary imperial *repertoire* to e.g., export "good governance". Considering global interconnectedness, capacity building in third countries contributes to the cyber resilience of the EU and is also an influential foreign policy tool in many other respects. In 2018, the Council of the EU issued guidelines on external EU cyber capacity building and stressed the role of cyber capacity building "in partner countries and regions as a strategic building block of the EU's cyber diplomacy efforts to promote and protect human rights, gender digital equality, the rule of law, security, inclusive growth and sustainable development, and as a key dimension of the EU's Digital4Development strategy".[130] The document

[126] European Commission, "Commission Recommendation on Cybersecurity of 5G Networks" (C (2019), 2335 final, Brussels, 2019).

[127] Council, "Council Document on Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of Malicious Cyber Activities" (6852/1/19, Brussels, 2019a).

[128] Council, "Preliminary Draft Reply to Question for Written Answer E-001005/2018 – Marietje Schaake (ALDE) 'Attribution of the NotPetya attack" (8641/18, Brussels, 2018a).

[129] Josep Borrell, "Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic," *Council of the EU*, 2020b, [https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/].

[130] Council, "EU External Cyber Capacity Building Guidelines" (10496/18, Brussels, 2018c).

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

refers to the 2015 Conclusions on Cyber Diplomacy and to the values and principles set out in the 2013 EU Cybersecurity Strategy, which "should serve as the underlying framework for any external cyber capacity building action",[131] and the EU appears to identify with the role of the moderator of economic and societal prosperity. It is advised, for example, that actions taken, and the common and comprehensive cooperation with international partners, reflect the understanding that existing international law and norms apply in cyberspace; fundamental rights and freedoms are protected and safeguarded by design; the strengthening of democratic and multi-stakeholder internet governance models; support for principles of open access to the internet for all; and that a shared responsibility approach be taken that entails involvement and partnership across public authorities, the private sector and citizens and promotes international cooperation.[132] Therefore, in its capacity building efforts the EU, arguably, aims at exporting these norms not forcibly but via proposing them for consideration, while building alliances to effectively resist and take on opposing or significantly diverging approaches of China or Russia. Indeed, as argued, major powers of the world seem to have serious disagreements about the conceptual core of cybersecurity,[133] and the EU evidently focuses on engaging in dialogues in different *fora* concerning the issue. At the same time, the entity now openly takes part in a cyber power competition both in technological and non-technological terms. At the international level, the EU's presence and push for influence is visible, for example, in the UN-associated platforms and during regional consultations with OSCE, the CoE, OAS, and ASEAN.

In December 2018, the UN General Assembly established a Group of Governmental Experts (GGE) on cyberspace in the context of international security, and, in June 2019, consultations were held with EU Member States. The GGE Chair summarised the exchange where "participants emphasised the need to highlight the opportunity cost of not having a functioning global internet and the increasing instability in cyberspace", great concern was expressed about "lower level ICT-threats".[134] Another central theme was the norms of responsible State behaviour, and

---

131 Council, 2018c.

132 Council, 2018c.

133 Anders Henriksen, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019).

134 United Nations, "Summary of Consultations with European Union Member States, 19-20 June, Brussels," Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2019, [https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf].

"participants stressed that norms agreed in previous GGEs should not be revisited and that progress be made on questions relating to their implementation", putting out practical suggestions that could show-case how a state is "implementing the voluntary norms of responsible State behaviour, confidence building and other measures recommended by previous GGEs".[135] Emphasis was placed "on the point that confidence-building measures […] can also serve important political functions, integral to formulating a common stability framework for cyberspace", and participants discussed "the moderating role of the EU in intergovernmental processes, that it should act as a force for good in the world and in the promotion of a rules-based and human rights-based cyberspace".[136] As a peculiar feature of the consultations, multi-stakeholder exchanges were held, engaging think-tanks and civil society representatives who discussed state-centric and civil society-centric pathways, expressing clear preferences for the latter, and criticism was expressed that the "EU needs to redirect its approach to steering change and better communicate the value of the EU's normative agenda, including through leading by example".[137]

On the strategic bilateral level, besides the more mature cyber cooperation with the US and Canada, the EU is also into projecting of its powers in EU-Brazil, EU-Japan, EU-Republic of Korea, and EU-India cyber dialogues, while, apparently, having a troubled cyber cooperation framework with China. In the latter situation, since "China has already become a fully-fledged European power",[138] the agenda is far more comprehensive and, evidently, includes the BRI (together with the 16+1/17+1), Huawei/5G, and the latest pandemic-associated issues. These processes are put in context with the words of Internal Market Commissioner Thierry Breton who noted that the EU "has the strongest industry in the world", adding that its "companies —big and small— provide us with jobs, prosperity and strategic autonomy" and that "[m]anaging the green and digital transitions and avoiding external dependencies in a new geopolitical context requires radical change – and it needs to start now".[139] This was in addition to the Commissioner's previous statement that "Europe[140]

[135] United Nations, 2019.

[136] United Nations, 2019.

[137] United Nations, 2019.

[138] Emilian Kavalski, "China's '16+1' is Dead? Long Live the '17+1'," *The Diplomat*, 2019, [https://thediplomat.com/2019/03/chinas-161-is-dead-long-live-the-171/].

[139] Thierry Breton, "Making Europe's Businesses Future-Ready: A New Industrial Strategy for a Globally Competitive, Green and Digital Europe," *European Commission*, 2020b, [https://ec.europ a.eu/commission/presscorner/detail/en/IP_20_416].

[140] Characteristically for many decision-makers who represent the EU's major bodies, Commissioner Breton, in fact, used "Europe" as a linguistic equivalent for "the EU".

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

has everything it takes to lead the 'big data' race, and preserve its technological sovereignty, industrial leadership and economic competitiveness to the benefit of European consumers".[141] Due to the above unease in the relations, we elaborate on cyber issues on the table with the Asia-Pacific region.

2. *Asia-Pacific focus of the EU: a cybersecurity context*

If ASEAN–EU relations, both actual and perceived, are the subject of one of the most productive segments of academic research on both sides, the EU's (as well as its Member States') activity on the Asia-Europe Meeting (ASEM), which came into existence in 1996, - is not generating much academic "excitement' in the European continent.

The EU needs to exhibit its persistence in order to project its strategic narratives and secure partnerships in the Asia-Pacific, which, as a broad region, has "grown up" geo-strategically in the most remarkable way since 1996. Therefore, in 2018, the EU announced its intentions to deepen security cooperation with Asia. The Council of the EU considered that among others, cybersecurity is a key area for enhanced security engagement, and outlined the immediate priorities and core elements of action, namely "[e]nhanc[ing] cooperation in the field of cyber security in favour of a global, open, free, stable and secure cyber-space" and "[d] eepening cooperation to investigate and prosecute cyber-crime in line with the Budapest Convention and work with Asian partners on the application of international law in cyberspace and the implementation of norms of responsible state behaviour and on cyber capacity building".[142] Later on, the ASEM Foreign Ministers' Meeting, chaired by Josep Borrell, issued a statement confirming these priorities, and also highlighting the need for protection of human rights and freedoms online, and adding the importance of development and implementation of confidence building measures in this area as well.[143]

The EU has been engaged in dialogues with strategic partners including political dialogue on cybersecurity and information society

---

[141] Thierry Breton, "Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence," *European Commission*, 2020a, [https://ec.europa.eu/commission/presscorner/detail/en/IP_20_273].

[142] Council, "Enhanced EU Security Cooperation in and with Asia" (9265/1/18, Brussels, 2018b).

[143] ASEM Foreign Ministers' Meeting, "Chair's Statement," Madrid, 2019, [https://www.consilium.europa.eu/media/41868/2019-12-16-asem-fmm-chair-s-statement.pdf].

dialogue with India,[144] cyber dialogue and dialogue on ICT policy with Japan,[145] cyber dialogue and information society dialogue with the Republic of Korea.[146] With both Japan and the Republic of Korea, the EU's geo-strategic "conversation" is supported by a Free Trade Agreement – on both occasions (with the Japanese side, the document is even called "Economic Partnership Agreement"), the relationships in trade can be evidently considered highly successful and mutually beneficial.[147] Nevertheless, cybersecurity is not trade, and two major common elements are present in the process: the focus on applicability of international law and norms to cyberspace, and combating cybercrime. Characteristically for this specific cooperation and its content, of these countries, only Japan is a member of the Council of Europe Cybercrime Convention (Budapest Convention), which serves as an effective framework for making a difference in practice.

Having experienced a decades-long period of predominantly positive interactions with ASEAN, the EU is now in the middle of implementation of the ASEAN-EU Plan of Action 2018-2022, in which, under the heading of 'Combating terrorism, transnational crimes, address other non-traditional security issues,' the two sides agreed to cooperate "on issues related to cyber security, including in combating cybercrime".[148] The EU's substantive engagement in cybersecurity is also visible within the ARF's framework. During the first cybersecurity-focused ARF meeting in Kuala Lumpur, on 25-26 April 2018, an initiative was tabled on creating practical avenues for consultation and information sharing among ARF participants on measures to protect critical infrastructure from malicious ICT acts, co-

[144] European External Action Service, "Fifth European Union-India Cyber Dialogue Takes Place in Brussels" (Press releases, Brussels, 2018b), [https://eeas.europa.eu/headquarters/headQuarters-home page/55452/fifth-european-union-india-cyber-dialogue-takes-place-brussels_da].

[145] European External Action Service, "Joint Elements from the 4th EU-Japan Cyber Dialogue – 11 June 2019" (Press releases, 2019b), [https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/64848/%E2%80%9Cjoint-elements%E2%80%9D-4th-eu-japan-cyber-dialogue-%E2%80%93-11-june-2019_en].

[146] European External Action Service, "4th European Union-Republic of Korea Cyber Dialogue Held in Seoul" (Press releases, Brussels, 2018a), [https://eeas.europa.eu/headquarters/headquarters-Home page/38995/press-release-4th-european-union-republic-korea-cyber- dialogue-held-seoul_en].

[147] European Commission, "South Korea" (2020f), [https://ec.europa.eu/trade/policy/countries-and-regions/countries/south-korea/]; European Commission, "The EU and Japan's Economic Partnership Agreement" (2020g), [https://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement/].

[148] ASEAN, "ASEAN-EU Plan of Action" (Manila, 2017), [https://asean.org/storage/2017/08/ASEAN-EU-POA-2018-2022-Final.pdf].

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

lead by the EU and Singapore.[149] In 2019, ASEAN and the EU issued a statement on Cybersecurity Cooperation predominantly focusing on the importance of normative frameworks, capacity- and confidence-building, and cooperation in general terms, and the mutual commitment to promote an open, secure, stable and peaceful ICT environment.[150] The two sides are engaged in a broader Information and Communication Technologies Dialogue, which, as the parties put it in a joint statement, can play an important role in promoting an open, secure, stable, accessible and peaceful cyberspace.[151] Cybersecurity continues to feature in discussions also with the new EU Commission and in conjunction with the EU's "New Strategic Agenda 2019-2024". In the context of solidifying the process of strategic narratives' formation, the document points out that the EU "must protect [its] societies from malicious cyber activities, hybrid threats and disinformation originating from hostile State and non-State actors", and "[a]ddressing such threats requires a comprehensive approach with more cooperation, more coordination, more resources and more technological capacities".[152] However, recent developments may create new challenges in the light of the EU's declared threat perceptions, its newly found plainspoken criticism and the inclination of several ASEAN members to sign up for the political vision of cyber sovereignty promoted by China.

Objectively, be it for the EU or any other major actor in the field of international relations, there is no easy answer when it comes to China-originated issues. In 2012, the EU and China managed to establish a cyber taskforce, but since then China has been perceived as one of the primary sources of cyber threats in Europe, and cooperation is focused mainly on confidence building measures.[153] As a particular feature of this relationship, the EU has been accused of applying double standards, because it appears to forget its principles on human rights, democracy and national minorities

---

[149] ASEAN Regional Forum, "Co-Chairs Summary Report, 1st ASEAN Regional Forum Inter-Sessional Meeting on Security of and the Use of Information and Communication Technologies." Kuala Lumpur, 2018, [http://aseanregionalforum.asean.org/wp-content/upload s/2019/01/ANNEX-12.pdf].

[150] ASEAN, "ASEAN-EU Statement on Cybersecurity Cooperation" (Bangkok, 2019), [https://asean.org/storage/2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf].

[151] Council, "Joint Statement of the 22nd EU-ASEAN Ministerial Meeting" (Brussels, 2019c), [https://www.consilium.europa.eu/en/press/press-releases/2019/01/21/joint-statement-of-the-22nd-eu-asean- ministerial-meeting/].

[152] Council, "A New Strategic Agenda 2019-2024" (Brussels, 2019d), [https://www.consilium.europa.eu/media/39914/a-new-strategic-a genda-2019-2024-en.pdf].

[153] Thomas Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain," *European Politics and Society* 19, no. 3 (2018), 321-337.

when dealing with China.[154] While there is a difference between claimed rights and granted rights, and the balance of power is a dynamic phenomenon which will always lean to one side, for example to the side of those who wield more economic power,[155] the EU's identity narrative as an advocate for the protection of human rights (online or offline) has not been notable in its dealings with China. Relations have rather been more compounded by the EU's empowerment to screen foreign direct investments from non-EU countries on grounds of security or public order, and the discussions around the strategic and legal implications of the potential reliance on Chinese technology in the rollout of 5G.[156] In the cyber taskforce's latest meeting on 13 January 2020, the two sides went no further than exchanging views on issues including the overall situation in cyberspace, international rule-making processes, 5G and the digital economy.[157]

On the ground, pre-Brexit and pre-pandemic EU-China trade averaged over EUR 1 billion a day.[158] However, the astonishing level of the EU's trade deficit with China —EUR 164 billion in 2019[159]— and the obvious lack of analytical comprehension on the EU's side of how China strategises its BRI in Europe where the EU is the power, were put aside by an indignation expressed by the Commission President. Ursula von der Leyen openly accused China of conducting hostile cyber operations and "a rise of online disinformation" against EU-situated entities and citizens, noting that "this cannot be tolerated".[160] In his turn, Josep Borrell has also painted a

---

[154] David Ramiro Troitiño, David, Tanel Kerikmäe, and Archil Chochia, "Foreign Affairs of the European Union: How to Become an Independent and Dominant Power in the International Arena," in *The EU in the 21st century. Challenges and Opportunities for the European Integration Process*, eds. David Ramiro Troitiño, Tanel Kerikmäe, Ricardo Martín De la Guardia, and Guillermo Á. Pérez Sánchez (Springer, 2020), 218 (209-230).

[155] Evert van der Zweerde "Democratic Repertoires of Political Legitimization," in *Russia and the EU – Spaces of Interaction*, eds. Andrey Makarychev and Thomas Hoffmann (Routledge, Taylor & Francis Group, 2018), 9-26.

[156] Kadri Kaska, Henrik Beckvard, and Tomáš Minárik, "Huawei, 5G and China as a Security Threat," *CCDCOE*, Tallinn, 2019, [https://ccdco e.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf].

[157] Ministry of Foreign Affairs of the People's Republic of China, "The 7th China-EU Cyber Taskforce Was Held in Beijing," 2020, [https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/jkxw_665234/t1731937.shtml].

[158] European Commission, "China" (2020h), [https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/].

[159] Eurostat, "China-EU trade in goods: €164 billion deficit in 2019," 2020, [https://ec.europa.eu/eurostat/web/products-eurostat-new s/-/DDN-20200320-1].

[160] Ursula von der Leyen, "Statement by President von der Leyen at the Joint Press Conference with President Michel, Following the EU-China Summit Videoconference,"

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

sobering picture about EU-China relations, explaining in an interview that "Europe has been 'a little naïve' in its relationship with China but its approach is becoming more realistic".[161] As a result, the EU's changed attitude towards China has been summarised in "Defending EU interests and values in a complex and vital partnership",[162] and this remains the *status quo* thus far.

VI. **Discussion and conclusion**

This paper's data-gathering was bound by an issue-specific claim to be tested – the idea to see whether or not the EU is in the process of utilising its inborn imperial paradigm to gradually become a globally-acknowledged power in cybersecurity, which can be considered an important element of the multidisciplinary debate on global geo-strategic redesign. The EU (as well as NATO, for example) does not belong to the Yalta-1945 international system, which objectively no longer exists. Indeed, there is a competition in the field, and the other contemporary empires, with or without acknowledging their high-profile geo-strategic status, are working to provide the world with a "single logic" on how to manage the cyber domain – the only thing is that, as noted, it is a matter of allowing a particular precedency to lead the way, but everything will be coming with a different set of ethics and political philosophy.

In the meantime, since the beginning of the 1990s, the world is "living" practically without an international system in place, there is still a need to communicate with different states and organisations. For a powerful actor like the EU, "communication" often has to be strategic, often synonymised with "cooperation" or even "enforcement of cooperation" – in scholarly terms, an empire's ultimate survival is always at stake. Keeping this premise in mind, a consideration that the postulates of Strategic Narrative Theory can be useful in the process of detecting the EU's actions on influencing the global cybersecurity environment is academically justified. Not many experts in the field will deny an important context-associated

---

European Commission, 2020a, [https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1162].

[161] Josep Borrell, "Europe Has Been 'Naive' About China, Says Josep Borrell," *Politico*, 2020a, [https://www.politico.eu/article/europe-has- been-naive-about-china-josep-borrell/].

[162] European Commission. "EU-China Summit: Defending EU Interests and Values in a Complex and Vital Partnership" (2020i), [https://ec.europa.eu/commission/presscorner/detail/en/I P_20_1159].

presumption that the EU has a certain range of capabilities to "produce" and, with a bit of time, solidify its own identity, system, and policy narratives on cybersecurity. However, this discussional framework needed yet another important factor to be analytically accounted for – the EU's cyber power.

In order to provide for a more nuanced way of data classification and a higher degree of measurability (now and in the future), this research proposed linking Strategic Narrative Theory with a model of dimensions of the EU's cyber power. Hence, after an elaborate review of the EU's communicative acts relating to cybersecurity, the detected narratives were classified according to what dimensions of cyber power they pertain to, and whether they are identity, system or policy narratives. The aforementioned dimensions made a nearly perfect analytical "deal" with the three types of strategic narratives producing a summarising issue-specific scheme where each and every EU cyber power-associated dimension is interlinked with a particular strategic narrative, and the whole construct is firmly "standing" on cybersecurity-focused strategic communication (see *Table 2*). In this way of looking at the issue, it is always visible what the EU has already delivered in the context of linking a desired integrated capability with a corresponding strategic narrative, and where the EU is still missing out in terms of reaching a cyber power's level. As an example of the latter, the cluster of the EU's "Integrated Government Capability" presumes that the entity has a strategy on attacking in cyberspace – the EU has not yet been able to formulate a strategic identity narrative on the point, although it has opted for a non-military approach in its 2017 cyber diplomacy toolbox.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

Table 2

Strategic narratives of European cyber power

The EU's strategic communication on cybersecurity			
Dimensions of cyber power / Strategic narrative	Identity narrative	System narrative	Policy narrative
	Attack and defend in cyberspace	*Delivering join actions; Share operational resources*	*Drafting policy positions; share operational resources*
Integrated Government Capability	— The EU is a coordinator — The EU is an autonomous player with technological sovereignty — The EU is a moderator of economic and societal prosperity (including protection of fundamental rights, in particular privacy and freedom of expression) — The EU as a force for good (Open and secure cyberspace is a foundation for economic prosperity) — EU is a space where a serious fight against cybercrime is effectively put up, while maintaining the highest level of protection of fundamental and human rights	— No cyber islands — "Whole-of-the-Union" — Complex web of horizontal and vertical policy interdependencies lead to formation of new alliances, rearrangements of old ones. — Thinking global, acting European: Fortress Europe	— Reducing uncertainty requires close cooperation ("there are no cyber islands") — Common and comprehensive action — Open and secure cyberspace is a foundation for economic prosperity (European Common Market is the foundation) and development — Cybersecurity entails a complex web of horizontal and vertical interdependencies with other policies — Hope for the best but prepare for the worse

The EU's strategic communication on cybersecurity			
Dimensions of cyber power / Strategic narrative	Identity narrative	System narrative	Policy narrative
	Work through international alliances and partnerships		
Integrated System Capability	— The EU is a civilizer and stabiliser: Changed security environment dictates the need for greater EU security autonomy and clear rules for the sake of predictability and economic development — The EU is a good model and moderator of economic and societal prosperity (including protection of fundamental rights, in particular privacy and freedom of expression) — EU as a force for good (Open and secure cyberspace is a foundation for economic prosperity) — EU is a global expert leader in advancing rules for secure and open cyberspace — EU is a reliable, strong and neutral partner in cybersecurity issues	— Cybersecurity is a complex strategic challenge — The EU is a significant cyber actor in the international system — Thinking global, acting European: Global Europe	— Complexities of cyber issues makes the EU perfectly well placed to act and support and coordinate, however the main responsibility remains with MS — System needs more trust frameworks, such as confidence building, predictable international normative frameworks, and capacity to cooperate and align action among partners (e.g., cyber capacity building) — Militarisation and non-friendly use of cyberspace by state actors (or by their proxies) needs a strategic response — Non-military cybersecurity policy is a real alternative

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

	The EU's strategic communication on cybersecurity		
Dimensions of cyber power / Strategic narrative	Identity narrative	System narrative	Policy narrative
	Using non-state cyber elements in direct support of policy (work together with infrastructure operators, software and hardware manufacturers, hackers, researchers, activists)		
Integrated National Capability	— The EU is a democratic, smart and structuring power: Multi-stakeholder approach is taken, which is the preferred model reflecting the realities of cyberspace; while with a systematic approach, the non-state capabilities can be harnessed (cyber competence networks, PPP *et cetera*)	— Cybersecurity is a shared responsibility, "whole-of-the-nation" approach: Multi-stakeholder system view is adopted, where private sector is essential, its capabilities are being harnessed User-level roles are important —"whole-of-the-society" approach—for example cyber hygiene	— Technological sovereignty Dependence on external providers is increasing the unpredictability of the cyber environment and exposes the EU to unnecessary risks. — Awareness raising at individual level supports a core collective capability.

Source: created by authors via adaptation of Klimburg; Dunn Cavelty; and Miskimmon, O'Loughlin, and Roselle.

Before the EU's 2017 Cybersecurity Strategy, which put forward a truly ambitious plan on enhancing international cooperation in creating effective cyber deterrence regardless of the sources of threats, EU-level policies on the theme were predominantly intra-oriented. Naturally, it pushed the cyber power's integrated system cyber capabilities to effectively work indirectly through economic policies of the world's biggest single market. In the external context, the EU used to rely on a number of reflectory international engagements, more specifically in the private sector. However, gradually, from a market-based and principled approach, the EU has arrived at a comprehensive policy that incorporates many elements from all major policy segments internally and externally including, on top of the narrow sectoral and internal market-oriented approaches, the Cyber Diplomacy Toolbox,

bilateral dialogues, involvement of the EU in international *fora*/conferences, cooperation with NATO, the UN, the CoE, OSCE, horizontal cooperation with non-state and hybrid organisations (FIRST, ICANN), which can be construed in terms of integrated system cyber capabilities. At the same time, when returning to Klimburg's clusters of cyber power, it is also clear that the EU has been paying attention to the constitutive elements, although not always as consciously as the theory would imply. The EU's cyber power as such remained contextual, depending on the depth of integration as well as the understanding of its own status as a powerful entity. There is also an issue of shifting responsibility in general cybersecurity, stating that the EU is just a coordinator, adviser, supporter, but the main responsibility lies with Member States and the private sector to secure cyberspace and build cyber resilience. However, the cybersecurity strategies of the EU and other high-level documents present a narrative mixing of "whole-of-the-nation" and "whole-of-the-Union" approaches.

Based on the data and analysis presented above, we can conclude with confidence that the EU bears significant cyber powers and these powers are growing. However, it also becomes clear that these are mostly "soft" in nature as the EU —as such— still lacks the 'hard' cyber capabilities. Some Member States have already developed significant operational capabilities in their national security context, but these are not yet in the common pool, and most member states are responding to the militarisation of cyberspace in kind, for example, developing cyber offensive capabilities.[163] Therefore, it is completely justifiable for the EU, which is not a military organisation, to put cyber power in its own context of strategic identity narrative, relying on its persuasive, normative and economic force, its subject-matter expertise and coordinating role. In addition, it is not across but very much along the line of the EU's "imperial" mission to export good governance.

The EU's views about the nature and structure of the cyber game have developed from cybersecurity being a technical problem to a complex strategic challenge with distributed forces, and which requires maximum efforts and a whole-of-the-Union approach. In this system, the private sector is also essential and its capabilities need to be harnessed on all fronts, and responsibility for ensuring cybersecurity shared among all levels. While information and communication technologies are key enablers of economic development, reliance on them can carry significant risks, and it is now emphasised that dependence on external providers is exposing the

[163] Agnes Kasper, and Csaba Krasznay, "Towards Pollution-Control in Cyberspace: Problem Structure and Institutional Design in International Cybersecurity," *International and Comparative Law Review* 19, no. 2 (2019), 76-96.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

EU to unnecessary risks. Facing increasing uncertainty is not possible without close cooperation at all levels as there are "no cyber islands," and common and comprehensive action is required, potentially deepening integration in new areas. Furthermore, the EU is portrayed as a democratic, smart and structuring power, taking the multi-stakeholder approach which reflects cyberspace realities and systematically building cyber capabilities from the bottom-up. In the cyber game the EU is clearly a moderator of economic and societal prosperity, based on protection of fundamental rights and open and secure cyberspace. While the EU, presumably, sees itself as a significant cyber actor in the international system and, evidently, argues that complexities of cyber issues make the entity well placed to act, support and coordinate, the main responsibility for cybersecurity is still pushed down to the Member States and the private sector (even to the citizens level, to an extent), emphasising a multi-stakeholder approach as opposed to the multilateral one. Focus on the importance of regulation, international law and norms, emphasis on the protection of human rights suggest that the EU is a civilising and stabilising force, but the changed security environment dictates the need for a greater EU security autonomy (or even strategic responsibility) and clear rules for the sake of predictability and economic development.

The EU, as such, remains undecided on the precise details of its "hard" cyber power. The entity's "imperial conversation" with the world revolves around the attractiveness of a rules-based and inclusive cyber-EU, a force for well-being and prosperity in the global village; however, tickets to this moral elite club may also be up for sale on occasion. Therefore, the EU's strategic system narrative can, in principle, allow the entity to react in accordance to its real might. However, it can also be observed that the appetite for pooling and sharing in regards of operational capabilities and "hard" cyber power increased, as in a technology-dependent society these are *condicio sine quibus non* of an effective policy. The EU communicates this via the carefully crafted "Thinking global, acting European" concept, which reflects the following two parallel strategies: lessening the vulnerabilities and decreasing the threats, being implemented respectively as increasing cybersecurity by shielding Europe from the harmful effects of global cyberspace and increasing cybersecurity by trying to reduce the threats originating from outside the EU by international norm setting and persuasion. In this process, the cyber fortress Europe is to be created, which by default needs to engage in empire-like behaviour if it was to insist on an open and free (and secure) global cyberspace. For the EU to have a convincing geo-strategic voice on the global stage, there is a need to understand and acknowledge what it really is as a power – let it be a cyber power to commence with.

Sobre los autores

La **Dra. Agnes Kasper** es profesora adjunta de Derecho y Tecnología en el Departamento de Derecho de la Universidad Tecnológica de Tallín (TalTech). Licenciada en Negocios Internacionales, tiene un título de máster en Derecho y un título de Doctora en Dirección de Empresas, y ha recibido cursos de capacitación oficiales sobre aspectos técnicos de ciberseguridad y pruebas digitales. La Dra. Kasper ha trabajado en embajadas, organizaciones de derechos humanos y ha dirigido el departamento legal en una empresa de consultoría y desarrollo de TI. También ha actuado en calidad de asesora en consultas con gobiernos sobre temas relacionados con la ciberseguridad, así como experta externa de la Comisión Europea. Su investigación actual se centra en los aspectos regulatorios de la ciberseguridad.

Vlad Vernygora es profesor de Relaciones Internacionales en la Universidad Tecnológica de Tallín (Estonia) y candidato a Doctor en Ciencias Sociales en la Universidad de Laponia (Finlandia). Es alumno de la Universidad Nacional de Derecho Yaroslav Mudryi (Ucrania) y la Universidad de Canterbury (Nueva Zelanda). Sus intereses académicos incluyen los imperios contemporáneos y sus narrativas estratégicas, la UE y sus políticas, las interacciones de Europa con Asia-Pacífico, la OTAN y sus socios mundiales, y la Iniciativa de la Franja y la Ruta. Vlad posee el Premio de Enseñanza de la Universidad Tecnológica de Tallinn de 2015 y una nominación preseleccionada para el Premio Nacional de Enseñanza Universitaria de 2016 en Estonia. Desde octubre de 2014 hasta abril de 2017, Vlad estuvo a cargo de la parte operativa del proyecto "NATO Global Perceptions – Views from the Asia-Pacific Region" del programa "Science for Peace and Security" de la OTAN.

About the authors

Dr Agnes Kasper is a Senior Lecturer of Law and Technology in the Department of Law of Tallinn University of Technology (TalTech). She holds a BA in International Business, MA in Law and Ph.D. in Management, and received formal trainings on technical aspects of cybersecurity and digital evidence. Dr Kasper served at embassies, human rights organisations and she was leading the legal department in an IT consultancy and development company. She has also acted in advisory capacity in consultations with governments on issues relating to cybersecurity, as well as an external expert for the European Commission. Her current research focuses on regulatory aspects of cybersecurity.

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, No. 65/2021, Bilbao, págs. 29-71
doi: http://dx.doi.org/10.18543/ced-65-2021pp29-71 • http://ced.revistas.deusto.es

Vlad Vernygora is a Lecturer in International Relations at Tallinn University of Technology (Estonia) and DSocSc Candidate at the University of Lapland (Finland). He is an alumnus of the Yaroslav Mudryi National Law University (Ukraine) and the University of Canterbury (New Zealand). His academic interests include contemporary empires and their strategic narratives, the EU and its policies, Europe's interactions with the Asia-Pacific, NATO and its global partners, and the Belt and Road Initiative. Vlad holds Tallinn University of Technology's Teaching Award of 2015 and a short-listed nomination for the 2016 country-wide University Teaching Award in Estonia. From October 2014 until April 2017, Vlad was managing the operational side of the NATO Science for Peace and Security Programme Project "NATO Global Perceptions – Views from the Asia-Pacific Region".

Cuadernos Europeos de Deusto
ISSN: 1130-8354 • ISSN-e: 2445-3587, Núm. 65/2021, Bilbao

Derechos de autor

Copyright