JM Atlantic Network 2

With the support of the Erasmus+ Programme of the European Union

Strategic Cultures, the EU, and Transatlantic Cyber Security

Joe Burton

This discussion paper was prepared within the framework of the Jean Monnet Atlantic Network 2.0. The European Commission's support for the production of this publication does not constitute an endorsement of its content, which reflects the view only of the authors. The Agency and the Commission are not responsible for any use which may be made of the information it contains.

JM Atlantic Network 2

With the support of the Erasmus+ Programme of the European Union

Strategic Cultures, the EU, and Transatlantic Cyber Security

Joe Burton

About the author

Joe Burton is Associate Professor of Cyber Security and International Relations in the School of Politics and International Relations, University of Nottingham. Prior to this he held a permanent position at the University of St Andrews and was a Marie Curie (MSCA-IF) research fellow at Université libre de Bruxelles (ULB), working on the two-year European Commission funded project CYBERCULT: Strategic Cultures of Cyber Warfare. He is the coordinator of the Jean Monnet Network, European Cyber Diplomacy (CYDIPLO).

Address: School of Politics and International Relations, Law and Social Sciences building - University of Nottingham. University Park, NG7 2RD – Nottingham, UK.
joe.burton@nottingham.ac.uk

INSTITUT D'ETUDES EUROPEENNES
INSTITUTE FOR EUROPEAN STUDIES

1. Introduction

In December 2020, the European Commission released its latest cyber security strategy.[1] The document sets the strategic direction for the EU and its member states on cyber security issues for the next 'digital decade' and is one of the most comprehensive strategic approaches to cyber security issues released by an international organisation or indeed any national government. The level of aspiration for a secure and prosperous cyber environment in Europe is notable, and the strategy seeks to build resilience in Europe, enhance member state capacity to respond to cyber security threats, and contribute to the wider global development of a safe and stable cyberspace. Despite its many positive plans for cyber security in Europe, the document lays out a series of steps to be taken by EU members that will prove challenging to implement and which continue to be fraught with controversy, including in such areas as encryption, digital and data sovereignty, 5G security, managing risk in cyber security supply chains, and developing a workforce in Europe to meet the massive skills shortages that continue to exist.

Meanwhile, in the US, the Biden administration has released its latest cyber security strategy in 2023.[2] The strategy is notable for its commitment to similar principles for a free and open internet, but which reflects the US commitment to its strategies of persistent engagement and defending forward, which are a much more aggressive approach to international cyber security which includes the regular use of hacking beyond US borders, including in allied networks, for strategic and political gain.

This article presents a comparative analysis of the EU and US cyber security strategies, identifying strengths and weaknesses and the issues that are likely to determine how effectively they are implemented. The overarching argument of the article is that the EU's cyber strategy emerges from a particular EU strategic cultural context which is based on the peaceful settlement of disputes, non-militarised approaches to cyber security, a preference for defensive and resilience building measures, rather than disruptive and offensive tools. While this largely defensively-oriented security culture may yield significant benefits and allow the EU to further develop as a distinctive global leader in cyber security, the approach appears to be increasingly out of sync with a global cyber environment, including the more assertive US posture. in which the use of offensive cyber capabilities has become commonplace. In such an environment, one of the central and ongoing challenges for the EU will be to reconcile it's defensive strategic culture and normative aspirations for cyber security with a more assertive role in countering adversarial actions through disruption and deterrence.

1. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy#:~:text=The%20EU%20Cybersecurity%20Strategy%20aims,benefit%20from%20trustworthy%20digital%20technologies.&text=Follow%20the%20latest%20progress%20and%20learn%20more%20about%20getting%20involved.

2. https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

The article begins with an assessment of the current challenges the EU and US faces in cyberspace, identifying five dynamics that have both driven the EU and US response to cyber security and will likely determine the success of their respective strategies. These are the underlying and ongoing cyber security pressures caused by the Covid pandemic, ongoing geopolitical challenges associated with the offensive use of cyber capabilities by the Russia and China, the diplomatic challenge, including negotiating wider international standards and norms, an economic and industrial challenge related to market dynamics, including both supply chain issues and broader economic disincentives in the cyber security industry to create secure cyber software and hardware, and lastly, a technological challenge, linked to the convergence of cyber security technologies, especially the emerging Internet of Things (IoT) market, 5G, Cloud Computing, Artificial Intelligence (AI) and quantum computing. The article then moves on to an assessment of the EU cyber strategy, its points of divergence from the US approach, and the extent to which it reflects and has been shaped by the EU's strategic culture, and whether it is itself a strategic culture building tool. This section of the article argues that the strategy lacks clarity on some key issues, including the nature and scope of cyber resilience, the ways in which the EU can deter malicious cyber activity, the EU's approach to offensive cyber operations, especially in a CSDP context, and some challenges associated with regulating the global IoT market and quantum computing in particular. The final section of the article presents an analysis of how the EU might move forward on cyber security and reconcile its defensively oriented strategic culture with the offensive environment in which it exists, and the more assertive US approach, including through supporting the emergence of resilient security cultures across sectors in the EU area, denationalising cyber security policy, bolstering cooperation with NATO, a key for a for EU-US cooperation, and moving towards a more robust role for cyber in CSDP missions and operations. Such an approach, it is argued, can help the EU respond to the increasingly offensive and disruptive nature of cyber operations, whilst not adversely affecting global cyber stability itself.

2. The strategic context of EU/US cyber security – five key dynamics

The EU's new cyber security strategy was published in December 2020 at the end of an extraordinary year in European, US and global affairs. As the strategy itself notes, the covid pandemic led to approximately 40% of the EU workforce remote working, causing significant challenges for the cyber security of remote networks and protecting distributed networks and workers. The Covid challenge was also accompanied by an 'infodemic' of disinformation, in which malicious online content was deliberately circulated by both state and non-state actors for a variety of purposes, including to sow confusion about the origins of the virus, to instil distrust in people about the measures taken by their respective government to combat the pandemic, including the efficacy of vaccines. These wider social media dynamics emerged simultaneously with targeted cyber campaigns by hostile state actors and criminal groups, including efforts to hack computer systems to ascertain intellectual property related to the design and manufacture of vaccines, and cyber-crime attacks, such as phishing scams, for example, using Covid-related content to lure victims into compromising their networks. Perhaps the most concerning aspect of the recent wave of covid related malicious activity has been the targeting of the health sector itself, including most recently a major cyber-attack against hospitals in Ireland, which led to operations and other procedures being cancelled or delayed. The scope of cyber insecurity during and related to the Covid pandemic has been profound, with overall rises in malicious activity, including, for example, a 60% increase in 2020 in the number Advanced Persistent Threats (APTs) attacks targeting EU institutions and increases in attacks against VPN services especially prevalent.[3] The pandemic has also intensified concerns about the societal impact of cyber operations, which have been equally apparent in the US and EU contexts, including the use of cyber-attacks against critical infrastructure, such as the health sector, and has illustrated the spillover effects of a real life pandemic within cyberspace itself. The wave of covid related malicious cyber activity has further highlighted the low maturity of cyber security in the health care sector, a widespread challenge in the European and US context, the vulnerabilities of medical devices themselves, the wide array of entry points that can be exploited by malicious hackers to enter healthcare systems, and concerns over the security of patient data, including issues around anonymity and privacy related to healthcare applications.

3. CERT EU, Threat Landscape Report, June 11, 2011, https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

At the same time as the cyber-related challenges caused by the pandemic, geopolitical dynamics that existed before the pandemic struck have continued, and probably deteriorated further, during this period. Russia and China have continued to present particular challenges to cyber security in Europe and to the EU's partners in the US and elsewhere. China state-backed group Hafnium were formally linked by Microsoft to the attack on the Microsoft exchange server, which compromised 30,000 organisations in the US, and which hit many European organisations, including the European Banking Authority. Russian hackers meanwhile were linked to the Solar Winds hack, a compromise of US government and private sector organisations which has been described as an unprecedented act of espionage and which has triggered a major debate in the US about the efficacy of US cyber security strategy.[4] The challenges from non-state actors linked to China and Russia has been accompanied by criminal groups exploitative campaigns, including increasingly damaging ransomware attacks. The Colonial Pipeline incident, for example, in which a US energy facility was compromised and a criminal group were paid a ransom of 90 million dollars (most of which has been subsequently recovered by US authorities), has illustrated that criminal actors are having strategically disruptive effects across the Atlantic and are increasingly viewing critical infrastructure as a lucrative target for exploitation.

While Russia and China have shown a willingness to conduct large scale damaging cyber operations in this period, the EU's cyber security relationship with the US has also been strained. The Trump administration in particular presented a variety of challenges for European cyber security policy makers. During his tenure, President Trump disputed his own (and European) intelligence assessments of Russian hacking, called for his political opponents to be targeted by Chinese hackers, setting a dangerous precedent for foreign interference in elections, and fired one of his top cyber security advisors, Chris Krebs, ostensibly for telling the truth - that there was no interference in the 2020 election. While the Trump administration set a troubling precedent for cyber security at the head of the western alliance, the problems have not disappeared now that President Biden has assumed office. The US cyber security strategy, which continues under Biden administration, is based on 'defending forward' through 'persistent engagement' - i.e. on disrupting and deterring malicious operations at source and in adversary (and, when necessary, allied) networks. European cyber analysts have expressed unease about implications for digital sovereignty in this context, noting that new forms of consent for US intelligence operations may be needed,[5] and the potential escalatory effects of such operations have also been in focus.[6] Some have posited, for example, that the Solar Winds hack was a *response* to persistent engagement.[7] While Europe cyber policy is largely defensive, regulatory, and based on resilience to malicious cyber operations, the 'great powers' appear to have moved in a different direction.

4. https://www.lawfareblog.com/solarwinds-need-persistent-engagement

5. Smeets https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/

6. Jason Healey, The implications of persistent (and permanent) engagement in cyberspace, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz008, https://doi.org/10.1093/cybsec/tyz008

7. https://www.cato.org/commentary/strategic-implications-solarwinds

Ongoing tensions have also continued in international cyber diplomacy, in which European countries have played a prominent role. While here has been some recent progress - perhaps most notably a consensus report reached on eleven norms of state behaviour through the latest United Nations GGE process[8] - several problems remain. The first is cheating – some states are clearly signing up to normative commitments at the UN level while continuing to ignore them. As Eric Rosenbach, former head of cyber policy at the Pentagon, has said, "The Russians have repeatedly violated the terms of any agreements on cyber at the United Nations".[9] The credibility of cyber diplomacy at the UN level is harmed by this dichotomy. A second problem is that the organisations that are charged with negotiating agreements at the international level seem not to be up to the task – either because they lack expertise in this policy area, the lack of universal membership (the UN being the exception), competition between organisations over cyber security policy, duplication in functions provided by international organisations on cyber policy, and the emergence of a range of initiatives at the international level that are hard to keep track of and influence, especially by states with limited diplomatic resources. Here, the Paris Call, Christchurch Call, ICANN, ITU, UN, EU, ASEAN, GFCE, Global Commission on Cyberspace Stability (to name but a few), as well as a range of regional organisations (e.g. ASEAN, OASS, Caricom, African Union) all have a role to play, but the bewildering scope of internet and cyber security policy creates difficult and complex policy workloads, even for organisations with permanent professional staff like the EU and the US Department of State. The need for cyber diplomacy to incorporate the views, interests and influence of a broader range of stakeholders, including big tech and civil society groups, is apparent, but existing international organisations are not well designed to include them. The debates that are emerging around new technology alliances could yield progress in this area, and the EU could play a significant role in them, but they are also a reaction to the poor institutional design of existing international fora, and the need to move beyond them to effectively counter cyber threats and enhance international cooperation. These cyber diplomacy challenges are thus significant international governance challenges, which are only beginning to be addressed. The EU's ability to promote its values through its cyber diplomacy and policy frameworks is significant – the GDPR, for example, has had a wide ranging impact on privacy and personal data protections – but anti-democratic practices remain widespread, and the EU does not have the diplomatic capacity or power to shape the global cyber security environment on its own. It has also experienced pushback from the US on GDPR and the EU has levied major fines on the US for breaches of the GDPR framework.[10]

The diplomatic challenges for the EU and US in dealing with cyber security issues are underpinned by complex and intractable economic and industrial challenges. There are still widespread skills shortages in cyber security in Europe, for example. According

8. https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what

9. NYT article https://www.nytimes.com/2021/06/15/world/europe/biden-putin-cyberweapons.html

10. https://article27representative.eu/en-us/gdpr-compliance/fines/

to the new EU cyber strategy document, there are 291,000 post for cyber security professionals in Europe that remain unfilled.[11] Similar shortages exist in the US.[12] Education and training programmes are growing in number and 'capacity building' in cyber is becoming a growing industry in itself, but not at the pace to fill this yawning gap. At the same time, skewed market incentives in the tech sector continue to create intractable cyber security problems. The ongoing consolidation of the internet sector, for example, means that cyber-attacks are more wide ranging and costly;[13] the global prevalence of Windows operating systems was a key reason the Wannacry various spread so widely and did so much damage. Perhaps more problematic is that companies entering the digital space are driven by the need to release products cheaply and not on the basis of how secure the hardware and software is. This is a particular problem in the Internet of Things market, where the rapidly expanding number of internet devices, and the concomitate lack of security being built into their design, will create a vastly expanded attack surface for malicious actors. In this context, debates about securing the digital supply chain have taken on a new urgency in the EU context, and have led to calls for repatriating supply of digital goods, or indeed restricting supply to fewer and trusted partners.[14] Security issues for the EU in this area include dependencies on a particular supplier, state or non-state actor interference in the supply chain, either to restrict supplies or to sabotage networks components, and/or a lack of attention to product security.[15] Supply chain risks cannot be dealt with by technical measures alone and require broader human and managerial processes to be in place, as well as covering the life cycle of IT production processes, including design, development, production, integration and deployment.[16] The globalisation of technology markets, where many companies rely on foreign vendors and manufacturing, as well as the prevalence of insider threats, including counterfeit software and hardware that finds its way into critical digital infrastructure (as in the case of the VisionTech case in 2010 when 60,000 counterfeit devices were sold and subsequently deployed in US missile programs, radiation detectors and high speed trains) is also a growing problem.[17] Even with its significant regulatory powers, the EU faces a steep challenge in this area in the years ahead.

These problems will be further compounded by the complex and disruptive effects of emerging technologies on cyber security policymaking. In this area, the convergence of technologies that will affect cyber security in EU and the US countries is already having an impact. These include the proliferation of IoT devices, the number of

11. Ibid

12. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

13. Burton, Joe, and Clare Lain. "Desecuritising cybersecurity: towards a societal approach." Journal of Cyber Policy 5, no. 3 (2020): 449-470.

14. https://www.consilium.europa.eu/en/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/

15. https://cybertechaccord.org/cybersecurity-tech-accord-welcomes-eus-call-to-strengthen-ict-supply-chain-security-and-plans-for-eu-wide-cyber-defense

16. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

17. Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001

which is expected to rise to 25 billion by 2025 (with one quarter of those in Europe),[18] the application of AI in cyber offence and defence including the weaponization of automated cyber processes,[19] ongoing problems related to 5G (and the process towards development and integration of 6G technologies), including a lack of political convergence on 5G provision and the role of Chinese suppliers in Europe, the increasing use of cloud computing platforms, and the potential implications of quantum computing on cyber security. Taken together, these technologies present great opportunities for policymakers and are central to a number of EU policy agendas, including the Strategic Compass initiative, the EU's AI strategy, the evolution of the defence industrial sector in Europe, including PESCO, CARD and the EDA. They are also crucial to wider societal and economic progress in the EU area. However, competition over these technologies is intensifying, with the EU falling behind the US and China in their development and deployment. There is a worrying divergence in adoption of emerging technologies across the EU area, with some countries falling behind, and a comparative gap in investment in the EU area as compared to the US and China,[20] (especially when the investment made by US and Chinese tech companies is included) and despite a heavy technology focus in the latest Horizon Europe funding mechanism.[21]

18. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

19. J. Burton and S. R. Soare, "Understanding the Strategic Implications of the Weaponization of Artificial Intelligence," 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2019, pp. 1-17, doi: 10.23919/CYCON.2019.8756866.

20. https://www.iss.europa.eu/content/digital-divide-transatlantic-defence-cooperation-ai

21. https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/increased-cybersecurity_en

3. Strategic culture and the EU cyber security strategy – points of divergence from the US

This section of the working paper is focused on EU strategic culture and draws points of difference from the US. Strategy does not emerge from a political or social vacuum. Nor is it solely shaped by the strategic environment described above. It is conditioned by historical experiences, the language, ideas, behaviour, and beliefs of policymakers, and exhibits characteristics that vary across polities, countries and indeed international institutions. These interrelated dynamics, which can be understood as strategic cultures, have long been studied by International Relations scholars, including in an EU and US context. Building a cohesive strategic culture in the EU has also been a goal of European policymakers and several of the EU's new leaders have emphasised the importance of building a more cohesive EU strategic culture in recent statements.[22]

At its roots, EU strategic culture is *peace-oriented* – this stems from the long history of the European project founded on responding to the violence of World War 2 by encouraging cooperative practices, conflict prevention and mediation across the European continent. Although the EU has developed its security and defence functions, especially in the last two decades, most notably through the CSDP, but also now through a range of initiatives, including the European Defence Agency and European Defence Fund, and Permanent Structured Cooperation (PESCO) – involving collaborate defence capability development between the member states) - the EU maintains this peace-oriented culture, and there remains a broad reluctance across the continent to militarise the EU's role and functions. This culture (ideas, practices, beliefs about the EU's role) informs the EU's Common Defence and Security Policy (CSDP). CSDP missions are mostly oriented towards conflict prevention and countering 'soft' security threats (climate, terrorism, maritime security etc.) rather than war fighting. While the EU's appetite for developing its role in security and defence is apparent, its foundational liberal and cooperative strategic culture may act as a brake on it doing so, unlike in the US.

A second and related facet of EU strategic culture is the application of *soft power.* As Benjamin Zyla has argued, "Above all, the project of European Union integration was inspired by the application of soft rather than hard power. Thus, the EU's behavioural benchmark is the peaceful integration of Europe and the values that have accompanied this process".[23] Soft power – broadly understood as the power of

22. Burton, J. (2020). Rejuvenating transatlantic strategic culture: Towards a new Atlanticism. In S. R. Soare (Ed.), Turning the tide: How to rescue transatlantic relations (pp. 75–88). Paris: EUISS.

23. Benjamin Zyla (2011) Overlap or Opposition? EU and NATO's Strategic (Sub-)Culture, Contemporary Security Policy, 32:3, 667-687, DOI: 10.1080/13523260.2011.623066 p. 674

persuasion and attraction – is an integral part of the EU's policy environment and its external diplomacy. In particular, it lends itself to diplomatic processes over military ones and to the resolution of disputes using a broader range of instruments, including crisis management, diplomacy and economic measures (including regulations and development as well as more coercive ones, such as sanctions). Soft power informs the EU conception of 'security' itself, as a broader subject area, including economic, environmental and societal security, and a range of other non-military threats and challenges. Economic security has of course been particularly important in the formation of EU strategic culture going back its founding as an economic community. The US approach to cyber also emphasises soft power and the internet has generally been seen as a method for advancing it. However, the EU tends to see soft power as an influence in the absence of miltary cyber power, which stands in contrast to the US.

A number of other cultural characteristics inform EU policy making in the post-cold war era. Stenn Rynning, for example, taking a more realist approach to the concept, has argued that EU strategic culture is necessarily built around the notion of *restraint*[24] in international affairs because "strategic power and culture in Europe are predominantly national".[25] This leads to a cautious approach to policy at the EU level, especially in the area of common security and defence, and a focus on economic, social and even cultural instruments of power over military ones. According to this logic, the existence of an EU strategic culture is likely to be weak and subordinate to national cultures, interests and preferences. Per Norheium Martinsen takes a different view, arguing that the EU's strategic culture is based on the idea of *comprehensive security* – a desire to act comprehensively in international affairs through utilising all the levers of power (economic, social, legal, military etc.) to maintain peace and security.[26] This may help explain why the EU cyber strategy appears at least to be moving into the defence area as well as doubling down on economic and regulatory aspects of cyber security. According to Janne Haaland Matlary, such 'securitising' moves by the EU will likely be justified in EU discourse (including in strategy documents) in terms of the normative goals of the EU and through conflict prevention narratives.[27]

EU strategic culture is also predicated on *rules, norms and values* which are constructed though *legal and bureaucratic frameworks* that seek to secure compromise within and between EU members. In this sense EU strategic culture is inherently legalistic and bureaucratic. As Thierry Tardy argues, "This security culture reflects a certain way to handle crises, through a mix of civilian and military responses, a focus on rather short-term and consensual activities, almost always in support of existing state authorities, and

24. An idea which has also received considerable attention in the cyber security literature – see Valeriano

25. Sten Rynning (2011) Strategic Culture and the Common Security and Defence Policy – A Classical Realist Assessment and Critique, Contemporary Security Policy, 32:3, 535-550, DOI: 10.1080/13523260.2011.623057

26. Per M. Norheim-Martinsen (2011) EU Strategic Culture: When the Means Becomes the End, Contemporary Security Policy, 32:3, 517-534, DOI: 10.1080/13523260.2011.623055

27. Ibid p. 526

in accordance with international legal instruments and a set of values and principles."[28] Although the EU is often criticised for this, as at times it leads to inefficient and slow policymaking, this behaviour is deeply engrained in the EU and serves important purposes, including maintaining political unity and consensus on key issues, as well as creating legitimacy for EU actions.[29] In early generations of strategic culture scholarship, Colin Gray described a subculture in the US of legal professionals, "for whom the use of military force was anathema". A similar culture exists now in the EU bureaucracy.

EU Strategic Culture					
Peace oriented	Soft Power	Restraint	Comprehensive Security	Rules, norms, values	Legalistic & bureaucratic

A reflective or constitutive EU cyber strategy?

Is the EU's strategic culture reflected in the 2020 cyber security strategy? Is the strategy itself a tool to build EU strategic culture through rationalising cyber threats and forging a consensus view? And, is the emergence of a more unstable, aggressive and offence oriented cyber security environment in the US and elsewhere nudging the EU to a more assertive cyber posture?

The 2020 EU cyber security strategy is built around three pillars – *1.) resilience, technology and leadership 2.) Building operational capacity to prevent, deter, respond, and 3.) Advancing a global and open cyber space*. These three priorities for the EU appear to align with the core challenges for European cyber security outlined in the first section of the article, and they also signal the strategic cultural traits of the EU described above. The cyber resilience concept, which is broadly understood as minimising the impact of and recovering from cyber-attacks when they inevitably occur, is largely acknowledged as a defensive strategy. In order to achieve resilience, the assumption is that the EU can play a role in developing the technology necessary to achieve a resilient cyberspace in the EU area, and that it can provide leadership within Europe to achieve that aim, thus not overriding national member states interest in this area, but acting as a coordinator of policy. The theme of conflict prevention also appears prominently, and the EU's liberal values are clearly on show, reflected in the goal to advance an 'open' cyberspace "grounded in the rule of law, human rights, fundamental freedoms and democratic values."[30]

The scope of the strategy also reflects the EU's comprehensive security strategic culture identified above. First, it acknowledges the widening targets of cyber-attacks to include

28. Tardy T. (2019) The European Union and UN Peace Operations: What Global–Regional Peace and Security Partnership?. In: de Coning C., Peter M. (eds) United Nations Peace Operations in a Changing Global Order. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-99106-1_12

29. Matlary, Janne Haaland. "When Soft Power Turns Hard: Is an EU Strategic Culture Possible?" Security dialogue 37, no. 1 (2006): 105–121. P. 113.

30. European Commission - Press release, New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient Brussels, 16 December 2020

many of the sectors for which the EU has responsibility for, including "connected devices, the electricity grid... banks, planes, public administrations and hospitals" as well as "energy grids, railways... data centres, public administrations, research labs and manufacturing of critical medical devices and medicines, as well as other critical infrastructure and services."[31] The strategy also sees a role for the EU at each stage of the cyber conflict life cycle (before, during and after malicious activity) in "preventing, deterring and responding to cyber-attacks" as well as to "detect signs of a cyber-attack early enough and to enable proactive action".[32] The comprehensive approach of the EU to security issues is thus reflected in the scope of the strategy and its recognition of the wide ranging and holistic nature of cyber threats.

The growing vulnerabilities created by emerging technologies are also well-covered in the strategy, hinting at the comprehensive nature of the strategy, its responsiveness to the changing cyber environment outlined in the first part of this paper, and the EU's soft power culture. 5G, for example, is a prominent focus; the strategy contains the '5G toolbox' in appendix, a 'soft' regulatory tool to encourage and persuade members to adopt measures to mitigate vulnerabilities as they roll out their 5G infrastructures. The toolbox could be seen in a strategic cultural context as an example of Rynning's conception of restraint as described above – the toolbox does not bind states, and seeks to sidestep some of the controversies about countries adoptions of Chinese 5G technologies in their networks and the lack of national political convergence on this issue. The shift to recognising an array of emerging technologies and their influence on cyber security is also contained in references to "data and cloud, next generations processor technologies, ultra-secure connectivity and 6G networks", and the strategy refers to the role of Artificial Intelligence in powering new Security Operations Centres across Europe. These again appear to be based on defensive measures, including prevention, detection and response (although little detail is provided on response mechanism) to major cyber incidents, rather than having any offensive role.

The strategy suggests that the EU hopes to overcome some of the challenges created by the wider strategic context by putting in place rules and bureaucratic mechanisms, which, as described above, are an inherent part of its strategic culture. The strategy exhibits the EU's rule making functions in a number of new directives that member states are expected to adhere to. These include a revision of the rules as part of the production of a new Network and Information System (NIS) directive to better align cyber security efforts across the EU council and private sector, including in areas such as incident reporting and national supervision and enforcement and the capabilities of the respective 'competent authorities' for cyber security in each of the member states.[33] The EU's legislation on protection of critical infrastructure will also be reviewed and the strategy contains a commitment to introduce new measures including a 'network code' setting rules for cross border cyber security of electricity infrastructure, introducing

31. Ibid.

32. P. 23

33. P. 5

new regulatory frameworks for the financial sector to better protect against cyber-attacks, and establishing 'horizontal' rules to encourage IoT security.[34]

Securitising moves?

Are there signs in the strategy of the EU moving towards a more assertive role in its cyber security posture and policy? Is 'soft power turning hard'[35] in an EU cyber context? And does this mean a greater alignment between the EU and US approach?

Deterrence, as a concept and policy priority, a concept which appears much more prominently in US cyber policy history (although less so in its most recent cyber strategy) is certainly more prominent in the 2020 strategy than it has been in previous iterations (the term was not mentioned at all in the first strategy of 2013). However, despite being more commonly associated with military-strategic capabilities, the strategy makes it fairly clear that EU cyber deterrence will be based on defensive approaches and legal instruments and focused primarily on cyber-crime: as the strategy says, "Tackling cybercrime effectively is a key factor in ensuring cybersecurity: deterrence cannot be achieved through resilience alone but also requires identification and prosecution of offenders."[36] Certainly, there has been a focus on sanctions as a tool in the EU's cyber diplomacy toolbox,[37] although there is little concrete evidence that they change adversary behaviour. Deterrence through resilience has also received attention in the academic literature – this is the idea that the rapid recovery of networks will make adversaries reconsider the gains they will achieve from attacking or exploiting them. But the EU does not specify the type and form of deterrence that it wants to achieve, who it wants to deter, or how. The latest US cyber security strategy advocated the concept of layered deterrence,[38] thus bringing much more specificity to the deterrence concept, and there are emerging forms of comprehensive deterrence[39] involving a wider range of actors and instruments, which could be a good fit for EU strategic culture. There is clearly room for the EU to further develop its thinking on this issues and the strategy commits the EU to "further define its deterrence posture" – but this will mostly relate to "political, economic, diplomatic, legal and strategic communication tools against malicious cyber activity", leaving the purview of offensive and disruptive cyber operations to the member states.

The EU's incorporation of a more robust cyber intelligence framework is also noteworthy in this context. The strategy commits to facilitate the establishment of

34. Ibid. p. 6, p. 9

35. Matlary, Janne Haaland. "When Soft Power Turns Hard: Is an EU Strategic Culture Possible?" *Security dialogue* 37, no. 1 (2006): 105–121.

36. Ibid p. 15.

37. Moret, Erica, and Patryk Pawlak. *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?.* European Union Institute for Security Stues (EUISS), 2017.

38. See Layered Cyber Deterrence: A Strategy for Securing Connectivity in the 21st Century By Benjamin Jensen Wednesday, March 11, 2020, 1:55 PM https://www.lawfareblog.com/layered-cyber-deterrence-strategy-securing-connectivity-21st-century

39. BurtonCyber deterrence: A comprehensive approach? https://ccdcoe.org/library/publications/cyber-deterrence-a-comprehensive-approach/ NATO Cooperative Cyber Defence Centre of Excellence 2018

a member states' cyber intelligence working group within the EU Intelligence and Situation Centre (INTCEN). Again, there is no indication that this new capability will act offensively, and it will be focused on situational awareness and decision making, especially in the context of the attribution of cyber-attacks and the use of sanctions. Nevertheless, it does further move the EU into a more traditional defence and security function, and away from its more economic and regulatory approach.

Some of the language contained in the strategy indicates a process of securitisation of the EU's approach to cyber. Securitisation is a concept that emerged in the International Relations literature which denotes the use of certain discourse (speech acts) to justify emergency policy responses.[40] It has been very prominent in the US context. Although the hyperbole common to the cyber literature, media and policy world (cyber pearl harbors, digital 9/11s etc.) is largely avoided in the strategy, there is some securitising discourse present. The most pervasive is references to a European cyber "shield" to protect the EU area, which is mentioned in the context of establishing the Security Operations Centres and the Joint Cyber Unit. There are also references to "watchtowers" in the strategy, again invoking military/policing functions to describe cyber defence. The Joint Cyber Unit in particular has received attention in the academic and policy communities, while this new body will provide greater connections between the civilian diplomatic and law enforcement communities with defence (military) communities, it is emphasised that the unit would not "affect the competences and powers of national cyber security authorities" - thus again demonstrating the a culture of restraint that seeks to integrate EU efforts with national ones as opposed to overriding them.

Perhaps the most notable development in the EU approach to cyber in the defence and security realm are contained in parallel political and policy processes, including moves towards recognising cyber security more in an CSDP framework. The most notable of these is the EU cyber defence policy framework (2018) which included EU support for the development of member state cyber defence capabilities related to CSDP, the protection of CSDP communication networks, promotion of civilian-military cooperation in cyber and joint training and exercises with partners including NATO.[41] The newly established policy mechanisms, PESCO, the European Defence Agency (EDA), and the European Defence Fund (EDF), are also developing stronger roles in cyber security. The EDA has established the "Demand Pooling for the Cyber Defence Training and Exercise support by the private Sector" (DePoCyTE) project, for example, which seeks, among other things, to develop a "common European cyber defence culture".[42] Although this goal is not specified or elaborated on further, it would appear to be in line with the formation of strategic cultures elsewhere, where individuals are socialised into a mode of strategic thinking, and through which a pattern of beliefs, behaviours and attitudes

40. For further discussion of the concept, see Joe Burton & Clare Lain (2020) Desecuritising cybersecurity: towards a societal approach, Journal of Cyber Policy, 5:3, 449-470, DOI: 10.1080/23738871.2020.1856903

41. https://eucyberdirect.eu/content_knowledge_hu/eu-cyber-defence-policy-framework/

42. https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

(in this case, about cyber) emerges.[43] Interestingly, this again indicates that EU cyber policy does not solely reflect European strategic culture, but seeks to instrumentalise it for EU political goals. The agency also aspires to help integrate cyber defence in the conduct of CSDP military operations and provide tools for situational awareness for command and control functions and digital forensics for military use.[44] The EDF has also taken a significant step into funding military cyber defence related projects in Europe through the European Defence Industrial Development Programme (EDIDP), which at the current time include projects on: Cyber defence platform for military networks (PANDORA); Tactical networks for cyberdefence (SMOTANET) and Cyber defence situational awareness (CYBER4DE, DISCRETION, ECYSAP), with an overall budget of around 100 million euros for digital and cyber projects.[45] As the EU is seeking to bolster its cyber security capacity in the military and defence sector, it appears to be focused still on defensive measures, capacity building, situational awareness, and there is no indication at the present time of a more substantive shift to the development and use of offensive capabilities.

43. Booth K. (1990) The Concept of Strategic Culture Affirmed. In: Jacobsen C.G. (eds) Strategic Power: USA/USSR. Palgrave Macmillan, London. https://doi.org/10.1007/978-1-349-20574-5_8

44. https://eda.europa.eu/webzine/issue18/focus/eda-s-growing-role-in-cybersecurity

45. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3325 see also https://ec.europa.eu/defence-industry-space/edidp-factsheet_en

4. Following the US lead? The EU as a more offensive, assertive cyber actor

The 2020 EU cyber security strategy certainly reflects EU strategic culture – its focus on soft power, norms, rules, defensive aspects, and resilience. But there are also some tentative signs that EU cyber strategy is changing – towards the EU becoming a more assertive actor with a higher level of ambition in the area of military defence and security, and an approach which would bring it more in line with the US approach. This is not a new process; EU leaders have over the last decade fairly consistently stated a desire for the EU to be a more capable security actor. Nor should it be assumed that this process results solely from the deteriorating international cyber security context – the EU's strategic environment – despite the structural explanation for this shift towards a more assertive role being plausible. The EU cyber security strategy also appears to act as a narrative tool (speech act) to justify and create political space for this more assertive role, and the securitising language is notable.

But is this new strategic direction sustainable given the inertia that EU strategic culture creates for EU security policymaking? If the EU wants to hold on to its more defensive, normative, peace-oriented ideas and behaviour, how can it further develop its cyber strategy whilst also responding to a more aggressive international cyber security environment? Can the EU continue to preclude EU level policies, doctrine or capabilities that would facilitate or encourage the adoption or use of offensive cyber capabilities?

Competency or culture - the denationalisation of cyber policy in Europe

The EU's central challenge in this area is to build multilateral policy that covers the European continent and which enhances its members cyber security. However, it must do so in a context in which its member states will be and are reluctant to cede responsibility for the military and intelligence functions of cyber security to the EU level (some of these tensions are ameliorated in the US context by the federal system of government). At the present time the EU does not have the competency for integrated cyber offence functions, and that is one of the reasons why individual states are still in the lead. The EU's strategic culture of restraint in security and defence is also a contributing factor. Whether this is sustainable is debatable. Cyber security is not a unilateral field of activity and requires extensive cooperation, including in the military

realm. A continued disposition towards member states taking the lead for cyber policy leads to a variety of other significant problems for cyber security – the development of offensive cyber capabilities by some states not others in the European area risks capability gaps emerging, free riding problems (where some states rely on others for cyber operations, which can cause intra organisational disputes and resentment). The continued nationalisation of cyber policy in the EU area also precludes effective information sharing on cyber threats, and may lead to the militarisation of cyber security functions, where militaries and intelligence agencies take a lead role and through which the negative aspects of their own strategic (sub)cultures become more prominent in cyber policy; negative aspects of military and intelligence strategic culture includes the creation of security dilemmas (including a tendency to interpret cyber threats and responses through a military lens), a proclivity to use cyber tools instead of other diplomatic options in conflicts with other states and non-state actors, the use of cyber tools for excessive espionage or surveillance practices and the over-classification of cyber security activity. In building its values into cyber policy at an EU level, policymakers should recognise that a lack of national democratic oversight of cyber functions can lead to or exacerbate undemocratic practice. The division of responsibility between member states retaining cyber competency and effective EU-level multilateral cyber policy is also problematic because of the interconnected and interdependent attack surface in the EU area, in which much of the civil critical infrastructure including energy, airways, transport, data cable has shared dependencies across the EU area.

Enhanced cooperation with the US?

Although the EU and NATO have signalled a commitment to enhancing cooperation, including on cyber threats, this should not be seen as panacea for cyber security policy. While there is a natural incentive to cooperate – cyber threats cross the military civilian domains, and NATO is well placed to act in developing military capacity in this area in a way that could complement EU efforts - there are some problems too. The first is the potential for a strategic cultural clash between the two organisations – NATO cyber policy rends to reflect the need and aspirations of its most powerful members – the US in particular, and US strategic culture in cyber security is very different to the EU's – it includes, for example, a focus on persistent engagement of adversaries, much less restrained use of offensive cyber, the projection of cyber power globally, and cyber exceptionalism – the inherent belief in the winnability of cyber conflict and the US role as global cyber police function.[46] NATO cyber policy co-operation with the EU is also complicated by the UK's recent exit from the EU, and by Turkey's role in the organisation.

46. Paper under development = Joe Burton, US Strategic Culture https://www.bisa.ac.uk/members/working-groups/usfp/events/us-foreign-policy-research-seminar-series-cybersecurity-and

NATO also appears to be stepping further into a soft regulatory role in cyber security across the European continent. As per the NATO summit in Brussels in June 2021, the alliance's communique on member states enhancing the resilience of critical infrastructure is prominent. NATO members have committed to taking action across seven key areas For the EU specifically, an illustrative problem is its cooperation with NATO. There is certainly renewed momentum in NATO-EU cooperation on cyber, and a recognition on both sides that the military and defence aspects of cyber security issues need to be dealt with in tandem with the economic, social and regularly ones, but the cooperation is in its infancy, with little substantive actionable progress emerging, and with strategic and political cultures that do not always mesh together well.

5. Conclusion

The new cyber EU cyber security strategy constitutes significant forward progress in addressing this suite of complex cyber security issues and what it refers to itself as a complex threat environment. Immediately it highlights how cyber security is integral to European security, and picks out threats from devices, threats to banks, aircraft, public administration and hospitals as right at the top of the agenda. Notably, it also ties digital transformation to green issues, highlighting ways in which cyber can be part of efforts to become more resilient to climate change. In this respect it shows substantial differences form the US approach.

But there are many problems which remain. Resilience remains ill-defined and hard to do – look at the ransomware demands that are getting paid – this is not what resilience looks like. Protecting free elections and democratic processes is difficult to do when democracy itself is under threat in the democratic area in the EU and in recent years in the US. These is also outdated rhetoric in evidence across the Atlantic area, such as a cyber shield – these sorts of analogies aren't particularly helpful- shields can be stabbed around, punctured, disarmed. The EU and US strategic culture is connected here, btu also a barrier itself to effective cyber security policy. This brings us to the transatlantic pre-occupation with cyber deterrence. This will be very difficult to do – do we consider cyber criminals or state actors to be deterred or even deterrable? This will continue to be a challenge for US and EU policymaker.

Finally, the evidence of this paper has shown that the EU approach is deeply informed by its own strategic culture, and that this diverges from the US strategic cultural approach considerably. This strategic cultural divergence could be a significant thorn in the side of noggin US-EU cyber and digital cooperation.

About the Project

The Jean Monnet Atlantic Network 2.0 is a small network of six members that keep intense communication and joint activities on the Atlantic Basin. The Network also serves as a central arena for discussing globalisation and key major trends in the several Atlantic microcosms. By combining the national with the regional perspective, its research and debates take into account the different foreign interests and pressures, as well as a critical view on the possible roles and future of the European Union (EU) in the area.

It is the present link of a long chain of projects. In 2016, the project that established the first Jean Monnet Network on Atlantic Studies (jeanmonnetnetwork.com.br) sought to foster knowledge and co-operation among scholars and researchers on topics of fundamental importance for Atlantic actors in general, and for the EU, in particular. It involved a greater number of centres and universities.

Seven years later, still focussed on the original three broad thematic axes -Energy/Sustainability, Trade/Economy (International Economic Flows) and Security/Inequality-, the Jean Monnet Atlantic Network 2.0 represents a continuation and a rupture with the previous undertakings.

It intends to offer a wide, innovative and sometimes controversial view on Atlantic problems and the expectations on and scope of the EU activities relative to them. The papers in this series are a sample of its achievements.

FGV | INTERNATIONAL INTELLIGENCE UNIT

CIDE

CIDOB BARCELONA CENTRE FOR INTERNATIONAL AFFAIRS

iee INSTITUT D'ETUDES EUROPEENNES INSTITUTE FOR EUROPEAN STUDIES

IPRI

POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE

JM Atlantic Network 2

With the support of the Erasmus+ Programme of the European Union

www.jmatlanticnetwork2.com