POLICY IN FOCUS

STRATEGIC AUTONOMY AND CYBERSECURITY

Paul Timmers, University of Oxford and Rijeka University*
May 2019

Recent developments in cybersecurity and strategic autonomy

In the last two years, strategic autonomy has become "Chefsache". It has been referred to by world leaders from U.S. President Donald Trump to German Chancellor Angela Merkel, from Chinese President Xi Jinping to French President Emmanuel Macron. After tense NATO and G7 Summits in May 2018, Merkel said, "We Europeans must really take our fate into our own hands"[1]. When European Commission President Jean-Claude Juncker gave his 2018 State of the Union speech last September with the title, "The Hour of European Sovereignty", he argued that the time had come for the EU "to become more autonomous and live up to our global responsibilities"[2]. Last December, 18 EU countries jointly stated that the EU "must adapt its trade policy to defend its strategic autonomy", specifically referring to a range of fields including cybersecurity and AI. They also said that the EU must "ensure its technological autonomy by supporting the development of a digital offer and create global reference players"[3]. Recently, EU Security Commissioner Julian King and Merkel made a plea for a more differentiated debate on strategic autonomy[4].

All these statements articulate a feeling of acute threat to sovereignty and strategic autonomy. This is driven by a confluence of increased dependency on transformative digital technologies with the explosive growth of cyber threats and incidents. It is further exacerbated by rising international tensions in the West's relationships with China and Russia and in transatlantic relations (Figure 1). The US has been stepping up restrictions on Chinese foreign direct investment (FDI) in key technologies. Key areas include semiconductors, telecommunications, robotics and AI. Peter Navarro, the White House director of trade and industrial policy, stated that the US would otherwise "have no economic future". The EU adopted, in record time, a measure to scrutinize FDI, partially due to cybersecurity concerns[5]. It is in this spirit that the 2017 revision of the EU's cybersecurity strategy aims to "build greater resilience and strategic autonomy" with the strategic interest that "the EU retains and develops the essential capacities to secure its digital economy, society and democracy"[6].

---

* The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s). This article was originally written as a contribution to the European Cyber Diplomacy Dialogue, Florence, 28-29 Jan 2019 and has since been updated. The author would like to express his gratitude to the participants of the Dialogue and especially to Dr. Patryk Pawlak of the EU Institute for Security Studies for his insightful comments and suggestions. The usual disclaimer applies. This paper reflects the personal views of the author.

[1] See https://www.reuters.com/article/us-germany-politics-merkel/after-summits-with-trump-merkel-says-europe-must-take-fate-into-own-hands-idUSKBN18O0JK, accessed 4 April 2019.

[2] European Commission "The Hour of European Sovereignty". https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf (12 September 2018).

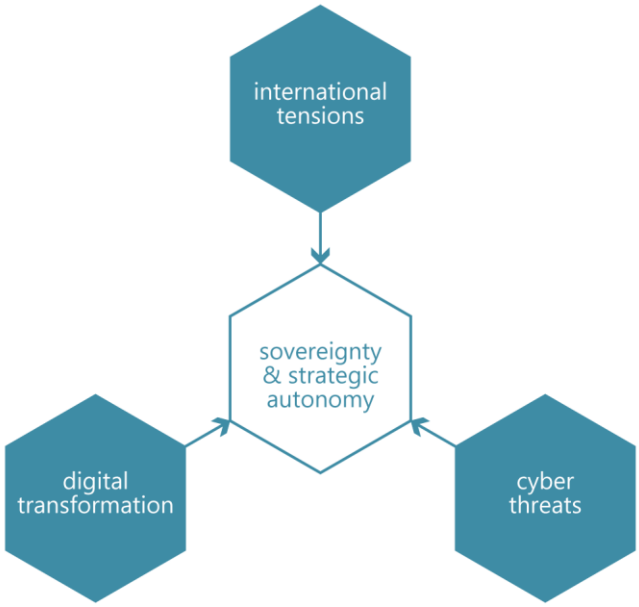
[3] Friends of Industry18 December 2018, https://www.bmwi.de/Redaktion/DE/Downloads/F/friends-of-industry-6th-ministerial-meeting-declaration.pdf?__blob=publicationFile&v=6, accessed 4 April 2019.

[4] Politico reported from their event on 16 Nov 2018: 'Security Commissioner Julian King said that Europe needs a "structural dialogue about what you might call 'dependency on infrastructure,'" which he called a "challenge for [Europe's] strategic autonomy."'

[5] European Commission. "Welcoming Foreign Direct Investment while Protecting Essential Interests" (13 September 2017).

[6] European Commission and European External Action Service "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017)250 final (13 September 2017).

As of today, however, there is little differentiation in the debate on sovereignty and strategic autonomy. This article aims to stimulate the debate on strategic autonomy and cybersecurity and contribute to the reflection on a more differentiated approach and international governance that includes cyber diplomacy.



What is meant by sovereignty and strategic autonomy?

Strategic autonomy is an ambiguous concept. Policy documents never truly define it; instead, they only rather vaguely refer to capabilities and the need to protect sovereignty. It doesn't even feature prominently in political science. Sovereignty, however, is a key concept in international relations and political science. It has to do with internal and external legitimacy, international recognition and authority and control over a territory[7]. Traditionally, in the Westphalian model, sovereignty was a matter of individual states (states being the units of the international system). Over the centuries, thinking and perceptions about sovereignty have evolved. Dealing with international issues by means of shared, pooled and delegated sovereignty has become quite common. Consequentially, a variety of forms of international governance have emerged, ranging from bilateral treaties to global multilateral arrangements.

Over the past years, several countries have also issued sovereignty claims regarding cyberspace. For example, [Cheung, 2018] summarises from a 2015 speech by Xi Jinping the Chinese definition of cyber sovereignty as 1) respecting each country's right to choose its own internet development path, internet management model and public policies on the internet, and 2) participating on an equal basis in the governance of international cyberspace, which requires states to "avoid cyber-hegemony and avoid interference in the internal affairs of other countries". In political science, there is no widely accepted and comprehensive cyber sovereignty doctrine yet.

Strategic autonomy and sovereignty are not the same. Rather, strategic autonomy tends to be seen by states as a means to realise their sovereignty. However, when the term "strategic autonomy" has been used in the past, it has nearly always come from military and defence circles[8]. France, notably, has a long tradition of using the term. Many recent analyses of strategic autonomy still focus on the military and defence perspective[9]. Yet as the statements of politicians and policymakers clearly show, they see strategic autonomy as a much wider issue. It is noteworthy that the most recent French Strategic Defence Review identifies threats to sovereignty in a broad sense and takes a wider view on strategic autonomy; indeed, it also discusses industrial and digital capabilities[10].

To bring more clarity to the concept of strategic autonomy, this paper puts forward the following definition: "Strategic autonomy is the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in the economy, society and their institutions".[11] [12] [13]

[7] Thomas J. Biersteker, "State, Sovereignty and Territory", *Handbook of International Relations*, Carlsnaes et al (eds), SAGE Publications Ltd (2012).

[8] The exception is India which used "strategic autonomy" to signify their independence from the USA, China and Russia (cf their leading role in the G77).

[9] Notably IFRI/SWP, "France, Germany, and the Quest for European Strategic Autonomy", Institut Français des Relations Internationals/Stiftung Wissenschaft und Politik (2017), https://www.ifri.org/sites/default/files/atoms/files/ndc_141_kempin_kunz_france_germany_european_strategic_autonomy_dec_2017.pdf; ARES "European Preference, Strategic Autonomy, and the European Defense Fund". Publication #22 (Nov 2017); Daniel Fiot, "Strategic autonomy: toward 'European sovereignty' in defence?". European Institute for Security Studies (November 2018), issue 12/2018; Hans Kundnani, "The Necessity and Impossibility of 'Strategic Autonomy'", German Marshall Fund (Jan 2018); Margriet Drent, "European strategic autonomy: Going it alone?", Clingendael Institute (Aug. 2018).

[10] DGRIS, 2017.

[11] Paul Timmers, "Cybersecurity is forcing a rethink of strategic autonomy", *The Oxford University Politics Blog* (14 Sept 2018). https://blog.politics.ox.ac.uk/cybersecurity-is-forcing-a-rethink-of-strategic-autonomy/, accessed 14 Sept 2018.

[12] This definition takes inspiration from IFRI – (Institut Français des Relations Internationals) which - in the narrower context of security and defence - identifies capacity and capabilities for political, operation, and industrial dimensions of strategic autonomy.

[13] Capability concerns knowledge and skills while capacity concerns the amount of resources. In cyber-diplomacy the notion of

According to this definition, the unit for strategic autonomy may be understood to be the state, but it is equally valid to consider an alliance of countries. For instance, France's former Home Affairs Minister Gérard Collomb talked of "Franco-European strategic autonomy". The definition is non-normative, though identifying "essential aspects" is of course a subjective matter. Finally, the focus on institutions rather than democracy makes this definition more universal as it can also be applied to nondemocratic regimes.

Cyber threats

There is no doubt that cybersecurity threats undermine strategic autonomy. Malware and DDOS attacks put critical infrastructures - from energy networks to industrial control and defence systems - at serious risk. Cyber theft of intellectual property, together with financial theft through hacking and ransomware, comes at a cost of hundreds of billions of dollars annually. States or state-sponsored actors display aggressive behaviour in cyberspace, global markets and foreign territories and they combine cyber and non-cyber interventions, such as massive foreign loans and strategic takeovers[14] that are perceived to be at odds with global open-market economy thinking[15]. The very nature of our democratic societies and values upon which they have been built are under threat because of election interference, whereby the freedom and fairness of the process can no longer be guaranteed with full confidence.

Cybersecurity is a driver of the rising interest in strategic autonomy. In "The Virtual Weapon", Lucas Kello shows that cyber aggression has three types of impact on the system of states[16]. Firstly, it upsets the power balance between states. "Cyber" is a new offensive technology that puts the defensive side at a disadvantage. Kello calls this *systemic disruption*. Secondly, states are able to reject accepted interstate behaviour by systematic and permanent harmful use of cyber intrusions and disruptions. This he calls *systemic revision*. Thirdly, the international state-based system itself gets challenged due to the entry of non-state actors, notably malevolent ones but potentially also powerful global tech companies, which implies *systems change*. States worry that their very sovereignty is at stake and Kello concludes that all three changes contribute to creating a "sovereignty gap".

Consequently, "cyber" has become a critical disruptor for the economy, society and the internal and external governance of states. However, it is also becoming a key force for defending these. More generally, mastery of digital technologies is an essential capability for future competitiveness, protecting society's values and bridging the "sovereignty gap". At this point, it is critical to note that even as approaches to strategic autonomy and the related governance are discussed, it is important to continue questioning whether strategic autonomy can become a reality at all in an era of rapid technological change and intelligent, agile cyber adversaries.

Pathways to strategic autonomy

How should governments deal with the challenge of strategic autonomy in the digital age? In particular, what should the approach to cybersecurity be in their domestic and foreign policies and what are implications for internal and external sovereignty? This paper proposes three possible approaches for responding to these questions (Figure 2). The first two, risk management and strategic partnerships, are state-centric and respond to systemic disruption and systemic revision. The third approach, promoting the common good, goes outside these frames and, building on a strong role of non-state actors in cybersecurity policymaking, it responds to Kello's systems change.

Each of these three approaches can be supported by specific action on promoting international norms and values in cyberspace. Countries promote such norms and values in multilateral settings such as the UN, the London process or the Paris Call for Trust and Security in Cyberspace. Companies do so too, such as with the Industry Charter of Trust[17]. Optimists hope these processes will safeguard global cyber peace. Pessimists say such efforts will, at most, buy time. Realists argue that non-binding international norms and values provide a supportive framework for any strategic autonomy approach. Given the specific attention to cyber diplomacy in this paper, the author also addresses international norms and values as they pertain to each

capacity building covers both capabilities and amount of resources.

[14] Tai Ming Cheung, "The Rise of China as a Cybersecurity Industrial Power: Principles, Drivers, Policies, and International Implications", *Journal of Cyber Policy*, Volume 3, Issue 3 (Dec 2018).

[15] Bundesverband der Deutschen Industrie (BDI), "Grundsatzpapier China" (10 Jan 2019).

[16] Lucas Kello, "*The Virtual Weapon and International Order*", Yale University Press. New Haven (2017).

[17] Siemens, "Charter of Trust on Cybersecurity". https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity.html, accessed 4 April 2019.

of the three strategic autonomy approaches that are presented next.

Figure 2. Strategic autonomy approaches

Risk management for cyber resilience (coping)

Following the risk management steps of "identify, protect, detect, defend, recover", governments could strengthen each step to the maximum in order to strengthen strategic autonomy. While absolute prevention would be ideal, many cybersecurity experts argue that digital systems are now so complex that keeping track of all components, hardening them and fully protecting against sophisticated attacks is impossible. Instead, they advocate focusing on rapid detection and defence combined with organised recovery in order to maintain an acceptable level of resilience.

Recognising that perfect protection is impossible, governments would have to invest in risk management that factors in an understanding that technology continues to evolve and that the adversaries are constantly trying new attack vectors. With that in mind, risk management is a possible answer and strategic autonomy becomes a matter of weighing costs and benefits. This approach underlies much of today's cybersecurity and privacy legislation and is usually acceptable for global business as well. Risk management is then combined with obligations to deploy state-of-the-art methods and technologies and to apply best effort.

Risk management assumes a certain level of residual risk. This is usually offloaded onto cyber insurance or - for very large, society-wide calamities - the government. At the same time, risk management enables governments to offload their responsibility onto the private sector since large parts of critical infrastructures tend to be managed by private companies.

In terms of policy, the risk management approach is well known: Governments impose risk management obligations, either hard (legal) or soft (self-regulation). Examples of legal obligations in the EU are the GDPR and the NIS Directive. Governments can also provide tax incentives, state aid and direct financing to step up investment in better incident response mechanisms and the hardening of critical systems. Governments could create a buffer fund to cover large-scale cyber damages

Telecoms interlude

Telecommunications infrastructure is the gateway to much of the economy, society and democracy as a whole. Strategic autonomy concerns are two-fold: 1) A telecommunications failure (possibly caused by a cyberattack) might have a highly disruptive and even catastrophic impact on the economy and society*; telecoms infrastructure could conceivably be weaponised with a kill-switch; 2) cyber intrusion in telecoms may remain virtually invisible yet be systematically exploited for years for intellectual property and data theft across the entire economy and society. The first concern may be addressed in several ways. One could analyse risks and "containerise" foreign telecoms equipment by allowing it to be used, at most, in non-critical parts of the telecoms infrastructure such as outside the core network. This is an example of risk assessment/risk management in the sense that it assesses where strategic autonomy matters most. Recently, the European Commission issued a Recommendation on cybersecurity of 5G networks which focuses on exactly this type of risk assessment and risk management**. Alternatively, in cyber-deterrence thinking, one would look for a prevailing counterstrike demonstration*** that may be considered a form of strategic interdependence. Addressing the second concern may require full strategic autonomy control, i.e. an independent supply of critical telecoms technology based on a strategic partnership. Alternatively, one could address this concern through other means of protecting IP and data, such as at an operating system level or with strong encryption. This, too, could possibly require strategic partnerships in addition to public policy geared toward improving the cyber hygiene of companies and research centres. The debate continues…

* Nick Bostrom, "Vulnerable World Hypothesis", Oxford working paper (2018), https://nickbostrom.com/papers/vulnerable.pdf, accessed 4 April 2019.

** European Commission, "Cybersecurity of 5G networks", C(2019)2335 final (26 March 2019).

*** Mariarosaria Taddeo, "Deterrence and Norms to Foster Stability in Cyberspace" (2018), DOI: https://doi.org/10.1007/s13347-018-0328-0.

similar to provisions in some countries for natural disasters. This possibility was raised in the EU's 2017 cybersecurity strategy[18].

A risk management strategy may have many downsides for external and internal sovereignty. One question is whether it is technically feasible to anticipate potential risks to the extent that a catastrophic threat, such as a sovereignty-threatening intrusion or kill-switch, can be pre-empted (see interlude on telecoms).

Risk management can also suffer from tragedy of the commons or free riders: Who is really taking responsibility in large-scale public or semi-public critical infrastructures, or for content on social media platforms or industry 4.0 platforms with millions of users? Risk management is also traditionally interpreted as being applicable at the level of organisations and executed by practitioners for whom threats to sovereignty are out of their scope (see risk management interlude). Consequently, strategic autonomy can still be undermined even when a risk management approach is in place. Current risk management practices, which are often too lax, have left the door open to the hacking of electoral systems with state-sponsored fake news on social platforms, the serious impairment of critical public services, such as health or transportation (cf. the Wannacry NHS health, Ukraine energy and NotPetya logistics incidents), or the massive theft of intellectual property. Such incidents undermine government credibility and expose weaknesses in national defence and strategic autonomy.

Cyber risk management and cyber resilience are natural partners. Cyber resilience is similar to the widely accepted concept of resilience against natural disasters. Therefore, risk management is an approach that may lend itself quite well to international diplomacy, provided the framing is around a shared interest in resilience. This may sound like a rather technocratic and pragmatic approach, but it is supported by actual cyber diplomacy today, which seeks to deliver agreements on international norms and values as well as responsible behaviour. Examples of such agreements are the Paris Call for Trust and Security in Cyberspace and its non-binding commitment to "prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure" and the 2017 G7 statement with a similar intent.

Strategic partnerships (win-win)

The US and China, as individual countries, may be the only ones with sufficient resources for strategic autonomy in the key technologies of the digital age (AI, cybersecurity, Industry 4.0 technologies, etc.). Other countries may have no choice but to pursue strategic autonomy as members of an alliance with like-minded parties, even if this may run counter to their national

Risk management interlude

In this article, the notion of risk management has been limited to cyber resilience. Here, risk management is more specifically defined as identifying, assessing and responding to cyber-related risks in critical infrastructures and essential services. It could be argued that the other two approaches in this article - strategic partnerships and global common good - also have to do with cyber-related risk management. However, risk management is usually understood in a rather narrow sense - as a notion originating from risk in industrial processes (standardised in ISO 31000) in which individual organisations are addressed but where the level of the state is outside the scope.

This more limited view of risk management is the approach followed in the often-referenced NIST framework for cyber risk management; it is also referenced by Europe's cybersecurity agency ENISA and the EU's NIS Directive*. Moreover, the cyber risk management obligation in the NIS Directive is limited even further to operators of essential services, including energy, water, transportation and providers of certain digital services like cloud services. Admittedly, by requiring a national cyber strategy and cooperation between national authorities, the NIS Directive applies to cyber risk management of critical sectors overall though without being very specific. However, in terms of risk management, neither the NIST framework nor the NIS Directive deals with cyber risks on a state or national level. Moreover, important sectors for sovereignty - media, defence and public administrations (the latter, unless being operators of essential services) - are left out.

This suggests that a wider perspective on risk management could emerge from mapping cyber-related risks against scope; where scope could range from individual organisations to non-critical sectors, to critical sectors of the economy and finally to the state as a whole. Next, an analysis could follow to identify the best fitting approach to strategic autonomy based on such a mapping of risks vs. scope. Such an analysis is the subject of further research and is foreseen for a separate publication.

* National Institute of Standards and Technology (NIST), "Cybersecurity Framework", version 1.1 (April 2018); ENISA, "Risk management", https://www.enisa.europa.eu/topics/threat-risk-management/risk-management, accessed 4 April 2019.

[18] European Commission and European External Action Service "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017)250 final (13 September 2017).

security instincts and even if shared governance implies relinquishing sovereignty to a degree.

The idea is that such a strategic partnership is a win-win situation. Earlier in this paper, the example of "Franco-European strategic autonomy" was mentioned. A modern understanding of sovereignty would not consider this an oxymoron. Taking an even wider view on the strategic partnership approach means also embracing strategic interdependency, whether with like-minded or not-like-minded countries[19]. In the military domain, a bilateral accord like the Intermediate-Range Nuclear Forces (INF) Treaty for nuclear intermediate-range arms control with mutual inspection between the US and Russia would be an example of strategic interdependency[20]. In the economic domain, free trade deals facilitate tightly integrated international supply chains. These can be considered forms of economic strategic interdependence. Sticking to the deal is win-win for all parties involved - and breaking it is lose-lose. Economic strategic autonomy must clearly also include the private sector, notably globally operating companies.

In many domains we have experience with quite profound strategic partnerships. NATO is a strategic partnership that is compatible with the military and defence perspective of strategic autonomy. In the economic domain, the SWIFT system of banks can be considered a rather successful strategic partnership. It maintains and secures the system of international financial transactions while respecting national financial autonomy. Thousands of private and public banks participate in SWIFT. Oversight is led by the National Bank of Belgium but shared closely with the central banks of G10 countries; there is also an arm's length involvement by central banks of other major economies, including China and Russia[21]. In "Digital DNA", Cowhey and Aronson draw lessons from existing global private-public partnership mechanisms, including SWIFT, to advance options for private-public cooperation in governance in the digital age. These lessons include flexible mechanisms, accountable authority, complementary governance arrangements and experimental problem solving[22].

Partnerships are also enabled by cybersecurity regulatory frameworks. For example, the third-country clause of the EU's Network and Information Security (NIS) Directive could be activated for a post-Brexit EU-UK partnership on cyber resilience. The EU Horizon R&D programme allows for wide involvement of associate countries, even for joint R&D projects in the sensitive area of cybersecurity[23]. In cybersecurity certification, the so-called Common Criteria Mutual Recognition Agreement already involves a range of developed economies. It could be envisaged to have mutually-recognised IT security certification[24] in some global supply chains, such as global shipping. To be relevant it would have to involve - in the interest of and probably driven by global business - countries as diverse as China, India, Japan, the US, UK, Brazil as well as the EU. If mutual inspection of certification proved impossible, could there be neutral third-party inspection? This would admittedly be quite ambitious, though, and would represent new territory for international cyberspace.

At first glance, strategic partnerships in a context of cybersecurity appear to be a promising route to pursue, especially for countries in Europe. But there are huge difficulties and pitfalls. To start with, it is hard to get parties to the negotiating table. Indeed, those parties represent a wide range of interests and very different cultural backgrounds; there are private and public actors, suppliers and buyers, border states and central states, large and small countries, etc. Secondly, in the low-trust field of cybersecurity, it is hard to share even basic information. Laying the groundwork with confidence-building measures may be necessary - an invitation to cyber diplomacy! Thirdly, even if a coalition of the willing - say, the EU - can agree on a common agenda, it may not matter when key players (the US, China) are not on board. Finally, one may doubt that each feasible partnership would have the financial clout to allocate the necessary tens of billions of euros for R&D in cybersecurity, AI, microelectronics, robotics, IoT, quantum technologies and Industry 4.0 (for an impression of investment in Industry 4.0 see Figure 3).

Matters are also complicated in terms of contents for strategic partnerships. One could argue that sectors most critical for daily continuity (e.g. essential services in cyber resilience frameworks[25]) and sectors essential

[19] Annegret Bendiek, "No New Cold War: Give Strategic Interdependence a Chance". *The Oxford University Politics Blog* (4 Dec 2018), https://blog.politics.ox.ac.uk/no-new-cold-war-give-strategic-interdependence-a-chance/, accessed 18 Dec 2018.

[20] Which, however, recently is at risk of breaking up.

[21] This is not to suggest that SWIFT is ideal. Dissatisfaction with US influence over SWIFT has in its nearly 50 years of history several times led to a crisis. Most recently, the EU has sought increasing its "financial autonomy" by setting up a "special purpose vehicle" for transactions with Iran outside SWIFT.

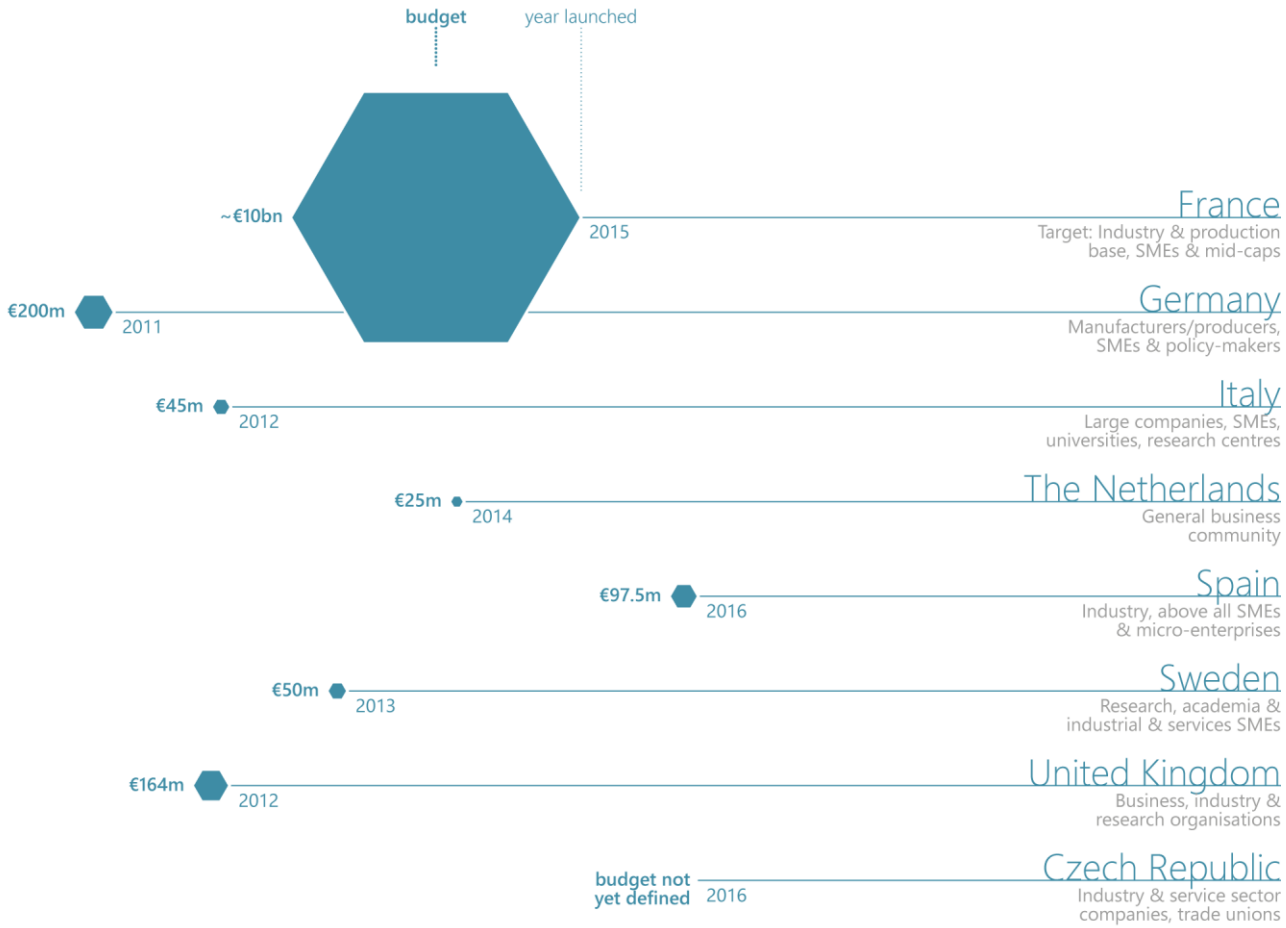
[22] Peter F. Cowhey and Jonathan D. Aronson, "*Digital DNA*", Oxford University Press, New York (2017).

[23] Subject to a project-by-project security scrutiny.

[24] The EU recently adopted the Cybersecurity Act. This provides i.a. a legal framework for cybersecurity certification in the Single Market.

[25] In the EU the Network and Information Security (NIS) Directive and cyber-related rules in sector-specific frameworks such as the Electronic Communications Code and the Regulation on Electricity Risk Preparedness.

Figure 3. Investments in Industry 4.0



Data: European Commission, "Key lessons from national industry 4.0 policy initiative in Europe". Digital Transformation Monitor. Brussels (2017).

for longer-term sustainability of sovereignty (defence, democratic, judicial and innovation systems) should both be addressed. And should strategic autonomy partnerships then not also build and protect intellectual property and innovation capability in the whole range of technologies mentioned before?

The sheer complexity and size of strategic autonomy topics and the wide range of choices for partnerships appear overwhelming. It may be tempting to take a pragmatic view: 1) Beginning with those alliances of like-minded countries that appear to work; 2) focusing on the topics that appear most pressing (such as 5G, AI and cybersecurity); 3) focusing on sectors of great economic interest to the partnership; and 4) mobilising as many resources as possible, i.e. being open to a private-public partnership approach. How to make these four points more operational is illustrated in the automotive interlude.

Pursuing a strategic partnership approach to strategic autonomy is a highly political matter. For one, it is necessary to understand who is "like-minded". Actors must also be able to steer the direction of partnerships and find common ground. Furthermore, they must do so while strengthening and embedding their own values (an example is the approach to ethics and AI[26]) and overcoming narrow sovereignty concerns. Such a political view can, as far as cyber is concerned, find its way into international norms and values for state behaviour in cyberspace. Clearly the strategic partnership approach requires a high level of engagement of cyber diplomacy.

Industry has provided guidance in this respect. An interesting reference was the position recently expressed by the Federation of German Industries (BDI). BDI subscribes to the liberal market economy, embraces multilateralism supported by organisations such as the World Trade Organization (WTO) and rejects China's

[26] Mariarosaria Taddeo and Luciano Floridi, "How AI can be a force for good:", *Science* 361(2018), 6404, pp.751-752.

state-led expansionism as well as the inclination of the US toward decoupling value chains[27]. Apropos of China, the European Commission and the External Action Service have recently also provided guidance, labelling China in different policy areas as a cooperation partner, a negotiating partner, an economic competitor and a systemic rival. They called for a differentiated approach of engagement, depending on the issues and policies at stake. This EU-China strategic outlook clearly suggests, without explicitly stating, that in areas in which Europe intends to pursue strategic partnerships (AI and batteries are mentioned), China is an economic competitor and not a partner[28], given its current market access restrictions.

Promoting the global common good

In the 1980s, a dramatic global challenge was identified: the growing hole in the ozone layer. In response, scientists, policymakers and industry joined forces to reduce the emission of CFCs, the chemicals that were breaking down ozone. Within two years, the Montreal Protocol was signed, CFCs were banned and - though it lasted many years - the ozone layer has started to recover. It was a major success in protecting the global common good, though it is seldom spoken of. Perhaps this story has lessons for protecting what many like to see as another global common good: an open, free, global and secure cyberspace.

The original internet was indeed a "free, open and global internet" available as a common good. Nevertheless, it came with a design flaw that is at least partly the cause of today's cybersecurity threats: It lacked security-by-design and privacy-by-design.

Internet protocols are open, internet technologies tend to be open source and internet governance is in principle world-wide and open to all. The origins of the internet were therefore not state-centric and not tied to sovereignty thinking. To be sure, there was *de facto* dominance of the US, but this was not by design. The internet community embraced decentralisation, openness and freedom.

Kieron O'Hara and Wendy Hall recently argued that the world is currently at serious risk that the internet will break up into a "splinternet" around four ideologies. State-centric sovereignty thinking and ideologies play an important role in driving this splintering[29]. But it has also been argued that, at the very least, the public core of the internet could be lifted out of the confines of national security and state sovereignty thinking[30].

This raises the question: Is there an alternative approach to resolve the conundrum of strategic autonomy and cybersecurity? Is there a way to simultaneously reinforce decentralisation and openness and security in the digital world? Can the world envisage making significant parts of the digital world available in an open, secure and decentralised way? Can cyberspace be seen as a global common good, cf. the recent appeal by Tim Berners-Lee[31], rather than slicing it up into isolated worlds under control of an individual state or a regional alliance of states? If the answer is positive, then state-centricity in cyberspace would be reduced. This would resolve concerns about strategic autonomy and sovereignty caused by cybersecurity risks.

This approach may not be applicable to all of the digitally-enabled world (not for defense…) but perhaps to several relevant parts. Could decentralised, open and cyber-secure approaches for example for smart grids, smart cars, smart health, and industry 4.0 be considered?[32] The answer is a qualified yes. It would require a combination of governance and technology. But, realistically, there will be serious questions about feasibility and effectiveness.

One governance approach is well-known namely, open source. The openness of the development of open source, the large community that can be involved, the related "libre" licensing all have shown to be able to deliver free, open and secure software, at least for some parts of cyberspace.

The weaknesses of open source are in the meantime well-understood (such as lack of quality control causing the HeartBleed incident of 2014, lack of financial means, dependency on a small number of individuals). They could be addressed by a combination of government policy and civil society – private sector -public collaboration. In the open source approach, the global open source and internet community as a collectives of non-state actors would play a major role. They would have to be involved as a recognised actor (which is not easy as it implies *systems change*, in Kello's terminology). Cyber-diplomacy engagement would be

[27] Bundesverband der Deutschen Industrie (BDI), "Grundsatzpapier China" (10 Jan 2019).

[28] EC and EEAS. 2019. "EU-China – A strategic outlook.", JOIN (2019)5 final (12 March 2019).

[29] Kieron O'Hara and Wendy Hall, Four Internets: The Geopolitics of Digital Governance, *CIGI Papers* No. 206 (Dec 2018).

[30] Broeders, Dennis. 2017. "Aligning the international protection of 'the public core of the internet' with state sovereignty and national security", *Journal of Cyber Policy*, 2:3 (2017), pp. 366-376, DOI: https://doi.org/10.1080/23738871.2017.1403640.

[31] Tim Berners-Lee, 12 March 2019, '30 years on, what's next #ForTheWeb?', https://webfoundation.org/2019/03/web-birthday-30/.

[32] To be very ambitious, could this also be pursued for IoT, AI, or quantum technologies?

crucial to explain the open source philosophy and build bridges between public/private sector and civil society.

A complementary, more recent option is distributed security control notably where many parties need to provide their validation of software or hardware. An example is provided by cybersecurity start-up Xage[33] which uses blockchain for distributed authentication of industrial control systems such as controllers used in the oil and gas industry - i.e. SCADA and industrial IoT systems. In this case security control is highly distributed and decentralised. If well-designed no state can exert cybersecurity control on these infrastructures (of course they could exert control by other means) nor do they need to fear foreign intrusion. Distributed security control can eliminate the tension between strategic autonomy and cybersecurity. However, distributed control is neither mature nor very well understood and as with open source, may appear threatening to those that are in a state-centric mindset as regards cyberspace. The state is, however, not replaced by any single powerful other actor. This option then does not imply "systems change".

The two options mentioned above can be promoted through government policy. Next to cyber-diplomacy as suggested this can consist of targeted public R&D funding that promotes open source and distributed security control, public procurement specifications, standardisation mandates, awareness raising and education, and even legislative measures such as for certification[34].

Governments could leave selected parts of strategic autonomy including cyber-defence to the private sector, such as to global tech companies. Obviously, this too would be a major shift in the state-based system of international order, i.e. *systems change*. Historically there are precedents to such shifts though there has always been a backlash and the recuperation of sovereignty lost to the private sector (an example is the East-India Company at the end of the eighteenth century). Witnessing the debate about digital tax and the breakup of "big tech", governments currently rather tend to increase their hold on sovereignty.

Conclusions

Each of the three approaches is still rough-cut at this stage and deserves further articulation. As European Security Commissioner King said: The EU needs a structural dialogue to understand where strategic autonomy really matters and to know how strategic autonomy would then be addressed. While three approaches have been presented here, as suggested in Figure 2 they do not need to be exclusive.

Automotive interlude

The automotive sector and related key technologies such as smart driving, batteries, and automotive cybersecurity should be considered for strategic autonomy, given the fact that transport is a critical infrastructure and given the huge economic importance of the automotive sector. However, automotive is a global industry with supply chains crossing geo-political divides. A car today is an integrated system with a huge number of components from a large range of suppliers. Global supplier and component qualification today are established practices based on contractual relations, industry-wide platforms and standards. In the ever-smarter cars, cybersecurity plays an ever more important role. Can cybersecurity then be handled within existing private-sector governance? Can one relax about strategic autonomy and leave matters in the hands of industry? Likely not. Cars of the future can be weaponised. Governments will want to be re-assured about the quality of the embedded cybersecurity. They possibly also want to be able, in the public interest, to tap into car data to track movements. Should a strategic partnership in automotive then be a mix of industry-led global cybersecurity certification and private-public SWIFT-like oversight?

Let's consider the case of the EU. Transport as a sector is subject to the cybersecurity risk management obligations under the NIS Directive. Battery technology for electric vehicles has been identified for a European strategic partnership approach, the European Battery Alliance, while competition with China is a major concern. The Alliance brings together "interested" EU countries and both private and public sector and kicked off with favourable investment support to capture a market of a projected value for Europe of €250 billion p.a. This provides an operational illustration of the points 1 to 4 made above for the approach to strategic partnerships namely: starting with likeminded partners, focusing in a pressing topic, in a sector of great economic interest and with a private-public approach to mobilise as many resources as possible.

AI is another area claimed for "Europe [to] become the world-leading region for developing and deploying cutting-edge, ethical and secure Artificial Intelligence". One cannot but wonder how this will apply to the automotive sector. As a case in point, in 2018 BMW and Baidu joined forces to accelerate autonomous (i.e. AI-based) driving. Baidu brings into this partnership Apollo, its open platform that "provides a comprehensive, *secure* and reliable solution that supports all major features and functions of an autonomous vehicle".

[33] https://www.ft.com/content/fe6930cc-8c29-11e8-bf9e-8771d5404543.

[34] Paul Timmers, "The European Union's cybersecurity industrial policy", *Journal of Cyber Policy*, 3:3 (2018), pp. 363-384. DOI: https://doi.org/10.1080/23738871.2018.1562560..

At this stage, a good view on current cybersecurity challenges is possible. It can also be identified whether these likely pose a strategic autonomy challenge. What is yet unknown is how to prioritize them nor what the best strategic autonomy approach to tackle these challenges would be. Neither is there a process for continuous assessment.

Many questions remain. For the next stage in the debate and as a suggestion for a structural dialogue, this paper proposes to focus then on providing the answer *at this moment in time* to the following questions:

1. Which approach is most applicable, for which strategic autonomy cybersecurity challenge?
2. How would a combination of approaches look like in terms of governance and resourcing?
3. How robust are the approaches in view of developments in technology[35] or in international relations[36]?

Answering these questions requires combining a dose of pragmatism with a political view on the future of the international order of states. Strategic industry relationships will influence interstate relationships and vice-versa and a workable compatibility between both will have to be achieved. As an example (see Automotive interlude), in the specific case of the automotive industry such compatibility has to resolve the potential tension between global automotive industry strategic partnerships and EU-China strategic interdependency (a strategic partnership of "like-minded" seems unlikely given EU-China systemic rivalry).

Finally, the analysis above identifies a series of concrete policy suggestions to address the sovereignty gap by reinforcing strategic autonomy. As said before, it may well be that a state or an alliance of states would pursue a combination of the three approaches. At least for the EU that would be the likely outcome of the desired structural dialogue.

Regarding risk management for cyber-resilience

1. Strengthen risk management obligations on a wider range of sectors
2. Provide tax incentives, state-aid and direct financing to strengthen cyber-resilience
3. Provide a buffer fund to cover large-scale cyber-damages
4. Address gaps in assigning responsibility and liability
5. Pursue cyber-diplomacy to adopt and implement do-not-harm norms for civilian critical infrastructures such as health, with measures such as information exchange and mutual assistance

Regarding strategic partnerships

1. Draw lessons from existing international private-public partnerships for strategic partnerships in the digital age
2. Activate third-country clauses in cybersecurity legislation for partnerships with likeminded states
3. Prioritize areas for strategic partnerships and operationalise these
4. Develop clearer and firmer political guidance for strategic partnering
5. Explain and advocate such guidance internationally through cyber-diplomacy

Regarding global common good

1. Strengthen private-public-civil society collaboration in open source; agree common agenda to address opportunities and weaknesses
2. For selected areas develop requirements for security-by-design and privacy-by-design
3. Support open source and distributed security control through R&D funding, multi-stakeholder collaboration, standardisation mandates, public procurement, and certification
4. Mobilise cyber-diplomacy to advocate the global benefits of open source and distributed security control

Paul Timmers is visiting research fellow for cybersecurity and digital transformation at the Center for Technology and Global Affairs (University of Oxford) and holds a visiting professorship at Rijeka University. He held various policy positions, including as Director of Digital Society, Trust, and Cybersecurity at the European Commission.

[35] Such as quantum computing that could break even high-grade encryption.

[36] Such as the EU being pre-occupied with internal problems.

EU CYBER DIRECT

This project is funded by the European Union.