Security Proofing the European & Transatlantic Tech Agendas

Discussion paper

Background

The Munich Security Conference (MSC) is the world's most prominent platform for the discussion of foreign and security policy. For nearly 60 years it has drawn attention to key challenges for the transatlantic alliance and global security. In this discussion paper, it raises the question of whether current technology policymaking across the transatlantic alliance takes key issues of national and international security sufficiently into account. Based on current examples it draws attention to the importance of assessing all policies and regulations for unintended effects on security and alliance cohesion and proposes the creation of a dedicated mechanism at the European level. The paper is a first attempt at outlining challenges and starting a debate. The MSC Technology Program welcomes feedback and contributions to the debate via technology@securityconference.org.

Summary

It has become common practice in many countries to carefully vet all new policies and regulations for their effects on climate change. From infrastructure funding to trade harmonization, European Union-level policies are increasingly becoming subject to "climate proofing." This makes sense, given the grave nature of the threat. But a warming planet is not the only existential challenge we face.

Our very way of life and the values on which our democracies are built are under attack. As autocratic challengers become bolder by the day, the guardians of our order are seemingly becoming more reluctant. This is why the EU needs a new dedicated Chief Security Officer, an official whose job would be to "security proof" everything the bloc does. Their one and only task would be to check whether key issues of national and international security have been taken into sufficient account in the formulation, negotiation and, ultimately, implementation of new policies.

Naturally, this is a tall order. Not only is the sheer number of policies to consider staggering, but the introduction of a new layer of bureaucracy is

inherently difficult – and often deeply unpopular. However, we must ensure that all new policies and regulations add to our security rather than subtract from it, that they do not weaken our alliance's cohesion or strengthen the forces of illiberalism. We must also ensure that legitimate considerations about taxation or competition do not crowd out equally legitimate concerns about security or geopolitics.

One obvious place to start is Europe's digital agenda and, by extension, the transatlantic technology agenda. Here, both the risks and the stakes are particularly high, and the need for sensible policies to be able to withstand any assault by illiberal forces is particularly obvious. The omnipresence of cyber threats pervades the digital sphere down to the level of individual users.

When it comes to digital policy, the conversation so far has centered on protecting European values and promoting Europe's economic competitiveness in the digital space. All these aspects are worthwhile — but layered on top of them should be a conversation about how to enhance security. Currently, potentially deleterious unintended consequences are still too often underappreciated – or worse, negative consequences are knowingly disregarded in pursuit of other aims.

Security remains European citizens' top priority for digital policy according to a recent survey by the Munich Security Conference, and they expect their governments to prioritize accordingly. The priority that Europeans give to the security of their digital life must also be a lens through which to view initiatives like the Digital Services and Digital Markets acts, the completion of the single digital market and the strengthening of Europe's digital landscape.

The goal of "security by design" should be applied not just to technology products but to digital and data policy, too. This means, at minimum, examining policies from every angle to ensure that they do not create unintended loopholes and problematic knock-on effects, or even increase the attack surface for those seeking to undermine the integrity and value base of liberal societies.

Unfortunately, examples of current EU policies that come with significant and, as of now unresolved, security risks abound. They range from the deliberate (and counterproductive) weakening of secure ecosystems to

insufficient safety requirements for Supervisory Control and Data Acquisition Systems on which most of Europe's critical infrastructure is run. What is obviously needed is an overarching mechanism within the European Commission to examine all pending and future pieces of digital legislation. Such a mechanism could run through the office of the proposed European Chief Security Officer, whose explicit responsibility would be to coordinate across the branches of the European policymaking process to ensure that compliance with the goal of security is maintained as legislation is developed.

Several countries, including China, proudly publicize how they are already integrating security in their wider tech and data policymaking. The EU must follow suit, as should its member countries, on both the national and sub-national level. An EU that carefully considers security will also be a more capable partner for the United States in pursuit of a robust, democratic transatlantic tech agenda that strengthens rather than undermines our position in the world and the values we stand for. And only by taking a stronger and more coherent view on security will the EU fully address the priorities and win the trust of European users.

The transatlantic digital agenda and the challenge of (dis)trust

Setting future standards for the governance of the internet, data, and digital technology has been a long-held ambition for the transatlantic partners. With new momentum toward a renewal of the transatlantic partnership, a window of opportunity has now opened to address this set of issues. The European Commission, beyond the new EU-US Trade and Technology Council, has envisioned a "dialogue on the responsibility of online platforms" and common solutions to antitrust enforcement and taxation in the digital sphere. The world is in a competition for the best approach to harnessing technology and the digital economy. If the world's democracies can agree on common rules and regulations strong enough to withstand the growing assault by illiberal forces, this would go a long way toward promoting a global digital order reflecting liberal-democratic values.

However, an EU-US tech agenda faces some significant hurdles. On the one hand, despite perceptions on some issues converging, substantive differences on digital policy remain. On the other hand, the asymmetry between Europe and the US (as well as other major powers) in terms of digital capabilities has given rise to an intense debate on European sovereignty in the digital space. The appearance of a push for European autarchy concerns

allies, especially in the US.

One underappreciated obstacle is the problematic lack of trust among European publics in the efficacy of government regulation in the digital sphere – both at the European level and particularly across the Atlantic. Europeans, so far, are not convinced that governments on either side of the Atlantic are able to provide sensible, robust, and most of all trusted guardrails to the digitalization permeating citizens' lives. That is the clear conclusion from surveys commissioned by the MSC in six European countries. Commission Vice-President Margrethe Vestager has said that the EU's strategy for a "digital decade" has to be "as much about building trust as it is about investing in digital innovation." If Europe and the transatlantic partnership are to live up to their goals for integration and cooperation in the digital sphere, they will need to address the trust deficit.

The nexus of trust and security

The surest way to do so is by putting security front and center. For Europeans, security is the essential element of a European, and by extension transatlantic, agenda on digital technology. Their overriding concern by a wide margin, the MSC survey finds, is that they themselves are secure when using the internet (38 percent of respondents across Europe name security as their top priority for digital policy), and they expect their governments to prioritize accordingly. Nearly half of Europeans say their governments are not taking enough action to protect their data. That is particularly pertinent against the backdrop of an "age of perpetual cyberconflict" that is not just exemplified by high-profile state-sponsored hacking incidents like the cases of SolarWinds and Microsoft Exchange. Rather, the omnipresence of cyberthreats pervades the digital sphere down to the level of the individual user.

Taking current debates on mobile device security as an example: the security of individuals' mobile devices has become a prerequisite for enabling their everyday digital and physical lives. They have become widely trusted as repositories for biometric, financial, and other sensitive information. This is only possible because companies have designed mobile devices as carefully curated and therefore secure ecosystems – a prime example of how users' trust is built on security. For this reason, governments are increasingly urging technology companies to ensure that their products are "secure by design". In this context, regulation to the effect of breaking down the walls around such secure digital ecosystems by enabling so-called

"sideloading" could have unintended consequences. It may open the door to malware and ransomware attacks at a time when malicious (state or non-state) actors, whether their goal is infiltrating governments for intelligence or businesses for financial gain, increasingly target individuals and their mobile devices. This is why both private cybersecurity analysts and authorities like the US Department of Homeland Security and the EU's cybersecurity agency ENISA warn against mobile malware from third-party sources.

Such issues are well understood at ENISA and relevant national authorities on both sides of the Atlantic. During the 2021 State of the Union speech, European Commission President Ursula von der Leyen announced the launch of a European Cyber Defence Policy, including legislation on common standards under a new European Cyber Resilience Act. This illustrates that at EU level there is an overall recognition that a balance is needed between internal market and competition regulation on one hand and security and privacy protections on the other. Therefore, the priority that Europeans give to the security of their experience online must also be a lens through which to view initiatives like the Digital Services and Digital Markets Acts, the completion of the single digital market, and the strengthening of Europe's digital landscape.

"Security proofing" European digital policymaking

The debate on Europe's sovereignty and specifically strengthening its digital capabilities is necessary. A more digitally capable European Union will also be a more reliable and more confident partner in pursuing a transatlantic digital agenda. Front and center in the conversation are goals of protecting European values and promoting European economic competitiveness (e.g., through a focus on antitrust and taxation policy) in the digital space. All these aspects are worthwhile – but layered on top of them should be a conversation about how to enhance security in the digital space. Instead, however, potentially deleterious unintended consequences for security are at risk of going under-appreciated – or, worse, known negative consequences may be disregarded in pursuit of other aims.

The knock-on effects of European digital capacity-building for security at every level need to be accounted for: at the level of individuals' privacy and security, at the level of public trust in the security of the digital space, and at the level of government resources that need to be expended to provide security and oversight. For instance, where data governance is taken out of

the hands of foreign governments or oversight for the security of digital ecosystems is taken out of the hands of companies, Brussels and European capitals will have to step in with adequate mechanisms. In some cases, the need to replicate the level of security and oversight already provided by private companies may create a lot of pain and little gain for governments: the resources for mirroring functions at the European level that, for instance, the Federal Trade Commission fulfils in the United States for policing malicious software and other bad actors, as well as myriad other competencies, should not be underestimated.

New regulation always comes with a risk of overreach, unintended short-term consequences, and long-term negative knock-on effects, particularly in an area as fast-moving and complex such as technology. Therefore, the goal of "security by design" should be applied not just to technology products, but digital policy, too. Today it is common practice to examine the effects on climate change of most if not all European level legislation. From infrastructure funding to foreign and security policy, policies are already or may soon become subject to such "climate proofing". In the same vein, it should become the modus operandi for policymakers to "security proof" legislation on Europe's digital agenda. This means, at minimum, examining policies from every angle to ensure that they do not create unintended loopholes and problematic knock-on effects or even increase the attack surface for those seeking to undermine the integrity and value base of liberal societies. At best, "security proofing" would make it a litmus test for all measures toward strengthening Europe's digital capabilities whether they also contribute to security – at the various levels mentioned above and even in terms of Europe's position in an ever more competitive and threatening global technological environment.

Doing so would require a form of overarching mechanism within the European Commission to examine all pending and in-progress pieces of digital legislation. Such a mechanism could run through the office of a "European Chief Security Officer", whose explicit responsibility would be to coordinate across the branches of the European policy-making process to ensure that compliance with the goal of "security by design" is maintained as legislation is developed. In an ideal world, this process would not only consider the hard aspects of technology and cybersecurity but also softer aspects of geopolitical consequence, such as the implications of certain measures, policies, or regulations for transatlantic cooperation and the overall cohesion of the West.

Only by taking a stronger and more coherent view on security will the EU fully address the priorities and overcome the “digital distrust” of European users. And an EU that considers security every step of the way will also be a more capable partner for the US in pursuit of a robust, liberal-democratic transatlantic tech agenda that strengthens rather than undermines our position in the world and the values we stand for.

Imprint

Stiftung Münchner Sicherheitskonferenz gGmbH
Karolinenplatz 3
80333 Munich
www.securityconference.org
technology@securityconference.org

Visit our app and social media channels:
www.linktr.ee/MunSecConf

About the Munich Security Conference (MSC)

The Munich Security Conference is the world's leading forum for debating international security policy. In addition to its annual flagship conference, the MSC regularly convenes high-profile events around the world. The MSC publishes the annual Munich Security Report and other formats on specific security issues.