ECIS European Committee for Interoperable Systems

Summary
ECIS webinar on Digital Sovereignty & Cyber Security Resilience
1 December 2021

Jonathan Sage
Chair of the Public Affairs Group at ECIS

Jonathan briefly introduced ECIS, explaining that ECIS is a trade association which was established in 1989 and has been involved in a number of legislative initiatives – for example, the adoption of the Information Society Directive, the legislative proposal on the Computer Implemented Inventions Directive, various WIPO-related initiatives and has played central role in the Microsoft cases. Over the past year, ECIS' events and discussions have focused on digital sovereignty. Jonathan also outlined the relationship between digital sovereignty and cyber security resilience to guide the discussion.

Lara Natale
Moderator, EU Digital Policy Expert

Lara introduced guest speakers providing transatlantic perspectives, research and industry.

Peter Fatelnig
Minister Counsellor for Digital Economy Policy, Delegation of the European Union to the United States

Peter explained that digital sovereignty is the tech version of open strategic autonomy; no man is an island, we are all a piece of a bigger thing, we constantly interact, and no country is fully sovereign. Trade, security, travel and immigration connect us. Open strategic autonomy means 'to emphasise the EU’s ability to make its own choices and shape the world around it through leadership and engagement, reflecting its strategic interests and values.'

The keyword is openness. Peter mentioned that EU, as largest free trader around the word, has no intention to give up this trusted global value network. On the contrary, trade will remain our premier foreign policy.
The EU and its Member States want to work on:

- Resilience and competitiveness (strengthening the economy);
- Sustainability and fairness (reflecting our values); and
- A certain level of assertiveness and rules-based cooperation, showcasing how we want to cooperate.

Key steps to achieving open strategic autonomy would therefore be:

- Better products and services - what we have is not good enough, and we need higher standards and certification (HW/SW). EU Cybersecurity Certification Framework is a good example.
- Better systems (infrastructure) – crucial in our complex world almost everything is critical infrastructure, not only pipelines and water plants. Again, certification is the key. "Only what is measured gets done", and the NIS2 Directive makes our wold safer.
- Combatting threats passively and actively. CERTs, information sharing, decision making and action - at technical level, tactical level and political level. Transatlantic cooperation can be greatly improved here as CISA and ENISA/EUROPOL have no cooperation at operational level.

- The new EU Cyber Unit will bring greater cooperation between what is too often dispersed, and accelerate the decision making.

Hannah Bracken

Digital Policy Advisor, The International Trade Administration

Hannah outlined that in the United States, there is a highly collaborative partnership model in terms of the interaction and information sharing between government and industry to address cybersecurity threats. Initially developed with a focus on critical infrastructure, the NIST Cybersecurity Framework continues to be a useful tool for managing cybersecurity risk since it was first produced with the active engagement of the private and public sectors. The Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices. It was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. There have been adaptations of the Framework in a number of different countries, including in Italy, Israel, Uruguay, and we are aware of several other countries referencing the Framework in various ways, including Brazil, Canada, and Switzerland. There have also been translations into Bulgarian, Portuguese, Spanish, Italian and Polish among other languages.

The Privacy Shield and the ability to transfer personal data generally is a key enabler of our broader cooperation with the European Union. Of course, underpinning much of this is the fact that one of our shared values with the European Union is privacy. And while there are different legal systems and technical approaches to privacy, our values are fundamentally the same. Cybersecurity features heavily in how we collectively as societies, companies, and citizens safeguard this shared value of privacy. The United States is committed to working together with the Commission to quickly negotiate an enhanced Privacy Shield deal that addresses the Court's concerns.

With the emergence of data localization policies and other restrictions on data flows being considered around the world in the name of increased cybersecurity and protection of privacy, it is important to develop interoperable systems and frameworks that reduce barriers to data flows and trade and that align with best practices regarding data security, while facilitating the intercompany and cross-border data flows that underpin innovation and growth of the digital economy.

Regarding the U.S.-EU Trade and Technology Council (TTC), the Department of Commerce leads or co-leads on five of the TTC working groups: Tech Standards, Secure Supply Chain, ICTS Security and Competitiveness, Export Controls Cooperation, and Promoting SME Access to and Use of Digital Technologies. During the September 2021 TTC meeting in Pittsburgh, Principals from both sides of the Atlantic highlighted the importance of engaging diverse stakeholders. Delivering on the promise of enhanced stakeholder engagement, Commerce has since led a roundtable on export controls and organized a major U.S.-stakeholder roundtable on 18 November with more than 300 participants. Details about future events will be available on the Department of Commerce's TTC website, which also includes contact information that stakeholders can use to propose suggestions to the Commerce-led and co-led working groups.

Przemysław Roguski

Assistant Professor in international law, Jagiellonian University, Poland

Przemysław explained how digital sovereignty relates to cybersecurity. For example, Thierry Breton, the EU Commissioner for the Internal Market, stressed the need to increase our collective resilience. To do this, we must ensure our technological sovereignty in the cyber field. Our real strategic autonomy and ability to act will depend on our ability to master and develop cutting-edge technologies in Europe. The concept of digital/cyber sovereignty has a different meaning for different States.

He then examined the meaning of "sovereignty" from a legal point of view. For example, cyber sovereignty is mentioned in the context of internet governance and the need for national control, like in China and Russia. However, in Europe, we speak about "sovereignty" in the context of control of data in order to protect European data.

In addition, the question of how to ensure the security of ICT networks arises not only among Member States but in the wider international community as the United Nations.

Sovereignty in public international law denotes supreme authority within a given territory which covers:

- Independence in setting and enforcing legal rules applicable to persons within a territory;
- Control over national resources stemming from that territory; and
- Authority to set and enforce rules.

In order to mitigate the threats posed by malicious use of ICT, it is not enough to agree on norms and rules on how States should behave towards one another. It is also necessary to induce States to increase their resilience towards cyber-attacks. This is addressed by the UN Group of Governmental Experts' Reports of 2015 and 2021 and endorsed by the UN Open-ended Working Group on Cyber and the UN General Assembly.

Some words of caution:

- Positive obligations alone, especially if formulated as recommendations ("norms") rather than binding rules ("law") are not enough to safeguard state sovereignty.
- The failure (so far) to sufficiently regulate conduct through negative obligations leads to measures of self-help to safeguard sovereignty.
    - Increase of capabilities.
    - It leads to increase of control ("supply chain security", "sovereign internet").

Paul Timmers

Professor, European University Cyprus, University of Oxford, Cybersecurity, strategic autonomy and sovereignty

Paul followed Peter's discussion and elaborated on strategic autonomy. When we speak about our own choices, there are three Cs involved, capabilities, capacities and control over those. We can ensure strategic autonomy through three approaches: strategic partnerships, risk management or global common good.

When we look at cyber resilience at the EU-level, we speak about NIS, NIS2 Directives (which take risk management approach), Cyber Shield and Cyber Resilience Act announced for the next year (likely rather a strategic partnership approach). The question is with whom you can work together and what you need to have. If you look at autonomy as having means that is capabilities, capacity and control, in order to strengthen sovereignty, it includes what you need to have for cyber resilience, for example, threat information sharing. However, resilience is a necessary, but not sufficient condition for sovereignty.

To ensure strategic autonomy one approach can be to pursue partnerships. Looking at different partnerships, we have a coalition inside the EU (GAIA-X), EU-27, trans-Atlantic, global; public (core of government, critical digital infrastructures) plus private parties (selected IP) and knowledge.

New technology (multi-party computation, homomorphic encryption) can move the focus in data localization from security sovereignty to economic sovereignty. Control of algorithms that analyse these protected data will become hard-core strategic autonomy.

Strategic autonomy and sovereignty can at times also be dealt with in global collaboration, e.g. cyber-resilience of global public health (WHO). We should not lose sight of opportunities and necessity of working together for a global common good.

Jonathan Sage

Chair of the Public Affairs Group at ECIS

Jonathan provided an industry and ECIS perspective on the topic. A State makes choices – one of those choices is setting up its own technical standards or behavioural rules which is creating risk of isolating itself and weakening its cyber resilience. So the collaboration between regions, as well as the EU and the US, globally is fundamental.

Interoperability and standards are very important in cybersecurity as well. We need open technical standards within security technology. Also more open semantics and frameworks - open source is also being more widely used in cyber security - open standards, common semantic languages, technical standards are effective to allow systems to talk to each other. Finally, a risk based approach with strong incentives arguably works most effectively to raise cyber resilience. The US NIST cyber security framework is a good example of this - voluntary but it is voluntary with some fairly strict measures if you are a critical infrastructure provider.

Lara Natale

Moderator, EU Digital Policy Expert

Lara concluded the webinar and thanked everyone for the lively debate.

***