European Cyber Agora

Working Group 3: Enhancing Collaboration between the Tech Industry and European Governments

Conclusions and recommendations

Co-leads: Thomas Boué, BSA Software Alliance; Andy Garth, ESET; John Hering, Microsoft, Eneken Tikk, Cyber Policy Institute

The interconnected nature of cyberspace requires joint efforts to maintain a global, open, stable and secure cyberspace.[1] The European Union (EU) seeks to promote inclusive engagement where governments, civil society and the private sector, work together.[2] Reinforcing regular and structured exchanges with stakeholders is one of the EU strategic cybersecurity initiatives.[3] The Council has recently concluded that strengthening ties with the private sector would amplify the EU's ability to protect and promote a unified vision of cyberspace based on shared values and democratic principles.[4]

To build towards effective cooperation between governments and industry, this Agora Working Group sought to identify areas where governments and ICT industry share the same values and objectives, and thus may offer avenues for closer collaboration. The co-leads of this Working Group[5] believe tapping into the full potential of multistakeholder cooperation would require strategic alignment between cybersecurity stakeholders; an alignment that would not only create flexible and dynamic cooperation mechanisms and options but acknowledge shared values as well as benefits to be achieved together.

1 – ICT industry shares the vision of an open, free, global, interoperable, reliable, and secure Internet

The Euro-Atlantic vision of an open, free, global, interoperable, reliable, and secure Internet[6] is shared by many members of the digital industry across the world providing information and communications infrastructure, connectivity, Internet services, ICT hardware, applications, cybersecurity products and services as well as digital marketplaces and social exchange platforms.

1 The EU's Cybersecurity Strategy for the Digital Decade, page 22: To advance multi-stakeholder cooperation on cybersecurity issues, the Commission and High Representative, in line with their respective competences, aim to reinforce regular and structured exchanges with stakeholders, including the private sector, academia and civil society, underlining that the interconnected nature of cyberspace requires all stakeholders to exchange upon, and take their specific responsibilities to maintain a global, open, stable and secure cyberspace. These efforts will provide valuable input for potential key actions at EU level.
2 2030 Digital Compass: the European way for the Digital Decade.
3 The EU's Cybersecurity Strategy for the Digital Decade, page 23.
4 Council conclusions on the development of the European Union's cyber posture, 23.05.22, para 13.
5 The co-leads of Working Group 3 are Eneken Tikk, Senior Research Lead, Cyber Policy Institute (CPI), Andy Garth, Government Affairs Lead, ESET, John Hering, Senior Government Affairs Manager, Microsoft and Thomas Boué, Director General, BSA Software Alliance.
6 Declaration for the Future of Internet.

To take public-private partnerships to the next strategic level, it is essential to acknowledge the aspirations and directions that stakeholders share and recognize the differences that industry and governments have. For instance, successful implementation of regulatory frameworks like the NIS Directive requires different, yet complementary, contributions from governments and industry. Different perspectives from industry and governments have contributed to strengthening the security of 5G networks. Together, governments and industry can advance policy frameworks like the EU Cyber Diplomacy toolbox.

The ICT industry is instrumental in creating open societies, driving societal change and advancing democratic values. Operating across the world, the tech industry has more responsibility in promoting peace, security and democracy today than ever before, as society becomes ever more reliant on technology to operate. Where governments set the rules, industry must respond and implement these in a proactive and sustainable way. In particular, the tech industry is on the frontline to uphold high standards of privacy and freedom of information, advance corporate responsibility, human rights, and fundamental freedoms and is taking proactive actions to accelerate the green and digital transitions and address the digital divide.

A prime example of this is how for over four years now, the Cybersecurity Tech Accord – a commitment of more than 150 companies to improving the security, stability, and resilience of cyberspace – has been advancing cyber hygiene principles and the adoption of vulnerability disclosure policies by technology companies. Signatories have also been vocal on the need for multistakeholder inclusion in the UN cybersecurity dialogues, and recently shared more insights on the role and responsibility of technology industry in the age of hybrid warfare. In the same vein, and against a backdrop of cyberattacks increasingly targeting essential services and infrastructures such as hospitals and energy facilities, a group of CEOs from oil and gas company pledged to enhance cyber resilience across the entire supply chain.

2 – ICT industry shares the goal of reducing the threats and risks in cyberspace

The ICT industry has witnessed, responded to, and mitigated against the threats and risks outlined in recent EU policy documents first-hand. Malicious and hostile cyber actors can exploit and erode trust in digital products and services. It is in the interest of both industry and government to share a high-level of awareness to understand the evolution and advancement of threats and threat actors who use ICTs for harmful purposes. Cyber related policy making must consider the realities of mitigating attacks and the process of response to contribute to cybersecurity ecosystems.

Recent examples illustrate how enhanced public-private collaboration can help in tackling cyber incidents and mitigate risks. In the context of the war in Ukraine, major cybersecurity firms have provided operational support to the Ukrainian government by moving key functions into a secured cloud environment. Leading European cybersecurity firms have collaborated with national

authorities and provided threat intelligence and information on ongoing cyber-attacks targeting critical infrastructures. Industry's threat assessments and trend observations complement the understanding of harmful ICT practices, while awareness raising campaigns help reduce their costly impact, for instance on risks posed by ransomware to organizations and users.

3 – ICT industry contributes to government efforts to maintain international peace, security and stability in cyberspace

Providing peace, security and stability primarily remains the responsibility of governments. However, enhancing cybersecurity and increasing resilience requires functioning public-private partnerships. Sustainable digital development requires the ownership and responsibility of industry and would not be possible without equal and transparent cooperation with governments. The many occasions of such cooperation – in threat intelligence sharing, dismantling botnets, thwarting cyber-attacks, patching vulnerabilities and securing supply chains – testify to the shared vision and common concerns between the public and private sector.

In an effort to protect their users and customer base, industry invests substantial resources in developing high-quality digital products and services, including resources to protect its online services. Industry also works with governments and customers to detect, prevent and mitigate threats to their accounts and data. Finally, industry shares interest in protecting civil society from cyber-attacks and their harmful effects.

4 – ICT industry can help shape global rules and standards

The EU has pledged to remain open to all companies complying with European rules and standards in so far as respective players will safeguard European values[7], fundamental rights and security and are socially balanced.[8] Industry shares the goals of connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms outlined in the Declaration for the Future of Internet. It is in the digital industry's and European governments' mutual interests to shape global rules and international standards in the field of ICTs.

Industry can be instrumental in this and increase the EU's competitiveness and resilience through standardization.[9] For instance, the 5G Infrastructure PPP works to have European industry driving the development of 5G standards and to develop and exploit at least 20% of the 5G standards essential patents. Also, the Coalition to Reduce Cyber Risk (CR2) *encourages government*

[7] See Press Release: EU and international partners put forward a Declaration for the Future of the Internet, Brussels, April 28, 2022; Press Release: Commission puts forward declaration on digital rights and principles for everyone in the EU, Brussels, January 26, 2022; https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695. As of June 1, 2022, the Declaration of the Future of the Internet has been signed by 28 states in addition to the EU Member States and the United States. See https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet. These states have pledged to be united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. They promise to welcome all partners who actively support a future for the Internet that is open, free, global, interoperable, reliable, and secure.

[8] Conclusions of the European Council of 1 and 2 October 2020.

[9] An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market, COM(2022) 31 final (Brussels, 2.2.2022).

regulators from all countries and all sectors of the global economy to leverage best-in-class international standards, such as ISO/IEC 27101 and ISO/IEC 27103, as the starting point for their approach to cybersecurity."[10]

Conclusions and way ahead

Mutual reliance, trust and cooperation between European governments and digital industry has never been more pertinent. We invite the EU to open a regular, encompassing dialogue and engagement base with industry. A strategic public-private partnership, one driven by shared goals and aspirations will help mitigate against differences that governments and industry, in their respective roles and perspectives, may have. The many processes in which governments and industry work together[11] demonstrate cooperation is already possible within defined and specific goals and intentions. The promotion of a value-based policy agenda able to shape technological development but also to address the fragmentation of the policy landscape and balkanization of cyberspace, is a priority for both parties.

By treating the public-private partnerships on an *ad hoc* basis or focusing on formalized collaboration only on technical/operational matters, both industry and governments miss opportunities to achieve shared goals and aspirations. While governments hold the mandate on security and set the rules in the public interest, industry needs to be able to adapt its operations and develop optimal market solutions alongside effective technical standards. An open and balanced dialogue is needed at both strategic and technical level to ensure trust and mutual reliance. Areas such as innovation, education, and skills development are also requiring enhanced public-private collaboration and a common approach towards shared goals and aspirations.

The way the private sector and governments have worked together to address the most pressing recent health and geopolitical conflicts are testament to the wide scale cooperation that is necessary and possible to solve new global challenges. Governments and industry need to build a higher level of trust and confidence, mutual understanding of the environment and goals they could serve. It is in the joint interests of government and industry to overcome the digital divide and prevent further destabilization of cyberspace. The potential benefits of mutual understanding and acknowledgment between governments and industry are many but trust, cooperation, equality, mutual accountability, and transparency is also required.

[10] Coalition to Reduce Cyber Risk White Paper on Seamless Security, 26 February 2020; https://www.crx2.org/seamless-security-white-paper-press-release
[11] European Cybersecurity Organization, Paris Call Community, the European Cyber Agora, UN OEWG and Cybercrime Treaty consultations etc.

The European Cyber Agora Working Groups 2022 are coordinated by

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Microsoft

The European Cyber Agora builds on the objectives of the EU Cybersecurity Strategy 2020 and aims to strengthen the ambitions of the EU in cyberspace based on a multi-stakeholder approach. In 2021, the Annual Conference highlighted four broad priority areas when implementing the EU Cybersecurity Strategy alongside the value of cross-sector input. In 2022, key stakeholders of the Agora community convened into four working groups to formulate actionable policy input for each area. The featured recommendations are the output of their consultations and research.