European Cyber Agora

Implementing the EU Cybersecurity Strategy

Recommendations From The European Cyber Agora

By Bruno Lété

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded by Guido Goldman (November 4, 1937 – November 30, 2020) in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

About the Author(s)

Bruno Lété currently serves as a senior fellow at The German Marshall Fund of the United States in Brussels. He provides analysis and advice on trends in geopolitics and on international security and defense policy. He focuses primarily on NATO, developments in Central and Eastern Europe, and cyber security.

Please direct inquiries to:
The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009

T 1 202 683 2650
F 1 202 265 1662
E info@gmfus.org

The European Cyber Agora 2021 is facilitated by Microsoft, the German Marshall Fund of the United States, and EU Cyber Direct.

Contents

About the European Cyber Agora

The European Cyber Agora is a multi-stakeholder platform that aims to bridge the gap between European governments, civil society and industry to advance the EU's cybersecurity policy agenda. It promotes collaboration across sectors, includes diverse voices, and champions evidence-based cybersecurity policymaking.

The European Cyber Agora builds on the objectives of the EU Cybersecurity Strategy, released in December 2020. The European Cyber Agora provides a platform for an inclusive discussion on cybersecurity in Europe and aims to build a more regular and structured multistakeholder engagement that will help advance European positions on the global stage. **The first European Cyber Agora convened online on June 2-3, 2021.**

European Cyber Agora 2021

500 Stakeholders

25 Partners

5 Plenaries

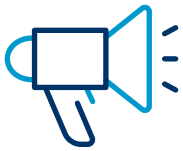
14 Workshops

Networking

Topics

- Digital Sovereignty
- Human Rights in Cyberspace
- Protecting our Healthcare
- Preventive Cybersecurity
- Cyber Peace Index
- 5G Toolbox
- Cybercrime
- Attribution
- Disinformation
- Critical Infrastructure
- Cyber Capacity Building
- Emerging Technologies
- UN Programme of Action
- EU Global Cooperation

How Can the European Cyber Agora Contribute to Policy?



Informing EU policy about evolving cyber concepts.

EU cyber policies, tools, and capabilities need to constantly adjust to technologies, societies, and geopolitics. The Agora discusses these evolutions in an ecosystem of diverse stakeholders.

Creating regular multistakeholder engagement for EU cyber policy.

Inclusive policy leads to solutions that are feasible and that are beneficial to all. The Agora can support more systematic consultations before and throughout policymaking.

Adding legitimacy to the EU cyber narrative.

The Agora presents an opportunity to showcase in Europe, and beyond, that multistakeholder input can solve complex cyber policy challenges.

Informing global players about EU Cyber Policy.

EU cyber power must be underpinned by global alliances. The Agora connects Europe with the transatlantic partners, and with all countries that share the value of democracy and safe and responsible cyberspace.

Leveraging a Multistakeholder Agora in the Policy Cycle

Summary: Implementing the EU Cybersecurity Strategy: Four Work Streams Recommended by the Agora Community

This report contains policy recommendations on cross-sectorial actions to implement the EU Cybersecurity Strategy. It draws from the multistakeholder discussions at the European Cyber Agora. The first part of the report finds that multistakeholder input would benefit all sectors, but policymaking still needs a different mindset. The second part concludes that multistakeholder input is a tool to support innovative, collaborative, and institutional policy solutions. The proposed working streams do not intend to exclude other areas of focus, but they can help to implement the EU Cybersecurity Strategy.

1 – Enhance Cross-Sectorial Lines of Communication

Strengthen the linkages between European cyber policy and non-governmental sectors. Create cyber capacity-building projects that familiarize scientists or researchers with policy planning, and host workshops or meetings to facilitate a discourse on how to match their analysis with policy engineering and policy solutions. ***(read more on p.13)***

2 – Support Civil Society's Engagement and Improve its Preparedness

Link cyber policy goals to operational civil society platforms that strengthen bottom-up responses to cyberattacks. Create a coordinated regular review of the digital society that measures the resilience of critical infrastructure, but also assesses the preparedness of societies and citizens. ***(read more on p.14)***

3 – Increase Operational Capacity to Prevent, Deter, and Respond

Improve the efficiency of the EU Cyber Diplomacy Toolbox by strengthening preventive cybersecurity initiatives. Facilitate the release of empirical data for researchers to advance data-driven accountability and incident analysis efforts. ***(read more on p.16)***

4 – Advance a Global and Open Cyberspace

Resolve the conundrum between EU commitments to open cyberspace and calls for strategic autonomy and technological sovereignty. Develop a credible narrative to convince third countries of the benefits of a democratic cyberspace, and the threat of a splintered Internet. ***(read more on p.17)***

Part One

The Relevance of Multistakeholder Input for the EU Cybersecurity Strategy

Part 1:

The Relevance of Multistakeholder Input for the EU Cybersecurity Strategy

Since its first Cybersecurity Strategy in 2013[1], the EU has come a long way. In these past years it has established a sophisticated policy framework around cybersecurity, centred on keeping actors accountable and upholding a concept of cyberspace based on international norms and rules. In the wake of the coronavirus crisis, and to bolster resilience against cyber threats, the EU presented in December 2020 a new Cybersecurity Strategy as a key component of Europe's digital future, along with the Recovery Plan for Europe and the EU Security Union Strategy. The European Commission also introduced proposals to address the cyber and physical resilience of critical entities and networks.[2]

The 2020 Cybersecurity Strategy combines three objectives. First, to increase the resilience and technological sovereignty of Europe. Second, to build operational capacity to prevent, deter, and respond to cyberattacks. Third, to advance a global and open cyberspace. These objectives reflect the EU's growing sense of understanding and ambition about the challenges faced by digital societies. It is a signal of its commitment to continue its global leadership on a wide spectrum of measures addressing current and future cybersecurity challenges. In this respect, the strategy also provides the EU with a unique opportunity to become a strong normative power in this field.

As cyberspace impacts the everyday life of all EU citizens, including their jobs, as well as businesses and industries, it is equally important to discuss the implementation of cyber policies within a broader community. The Cybersecurity Strategy calls upon the European Commission and the high representative to engage with all stakeholders, underlining the need for everyone who uses the Internet to play their part in maintaining a global, open, stable, and secure cyberspace. Yet, the strategy falls short of describing a clear blueprint on how to organize these consultations, or how to include them in policymaking. Neither does it specify what a dialogue between the public, private, and civil sectors needs to achieve to be useful.

In other words, there is still room to improve European cross-sectorial collaboration on cyber issues. The 2020 Cybersecurity Strategy acknowledges that multistakeholderism, underpinned by solid EU cyber cooperation and international strategic alliances, will lead to more stability and predictability in cyberspace. But a major shortfall in the strategy is the lack of a roadmap to harness nongovernmental expertise during the implementation process of cybersecurity policies. Rather than creating formal structures or procedures to do so, the EU needs to strengthen a mindset and environment of regular and open exchange across sectors. Otherwise, Europe is at risk of sustaining a situation where national authorities do not systematically gather and share information that is available from the private sector or other nongovernmental observers, which could help assess cybersecurity in the EU.

1 EU Cybersecurity plan to protect open internet and online freedom and opportunity, European Commission, February 7, 2013:
2 New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, European Commission, December 16, 2020

Yet, creating a diverse ecosystem would add legitimacy to the EU's cybersecurity policy approach across societies. Europe has a strategic interest to showcase to global democracies, and governments with a different political system, that multistakeholder engagement is the way forward on complex issues like cyber. Only by leading by good example, can Europe argue for more and deeper multistakeholder engagement within the United Nations, or toward other cyber powers such as China.

The key objectives of the new Cybersecurity Strategy would benefit from multistakeholder input. Cyberspace is a complex and interdisciplinary domain. It demands policy development that is inclusive and expertise-driven. Multistakeholder input does not mean that industry or civil society get to make decisions that should be made by governments. Neither does it mean that stakeholders need to be consulted on all issues all the time. But it does mean that when an issue is too challenging to be tackled by any one stakeholder group, all relevant stakeholders come together.

The Relevance of Multistakeholder Input for European Cybersecurity Policy

Intelligence and information gathering.

New ideas, analysis and problem solving.

Policy vetting and experimenting in an interdisciplinary ecosystem.

Monitoring the impact of policies, proposing improvements.

Building legitimacy for policies across European societies and in global processes.

Multistakeholder Input In Policymaking

Success Cases of the Past	→	Opportunities for the Future

Canada's Cyber Review Consultation Report

Between August 16 and October 15, 2016, the Canadian government organized an online public consultation that sought the views of Canadians, the private sector, academia, and other stakeholders on cybersecurity in Canada. This consultation was to provide an overview of cyber security trends and challenges, outline a way forward for cybersecurity in Canada, and solicit responses on 18 questions. In total, 2005 submissions through the web portal and 90 position papers were submitted. Throughout the consultation, several ideas were consistently raised as being important and relevant to cyber security in Canada. This consultation enabled the Canadian government to effectively identify several areas for future cyber action.

Australia's Consultations on Cyber Security Policy

The Australian Cyber Security Strategy 2020 was informed by extensive prior consultation. Between September 2019 and February 2020, government officials met with over 1,400 stakeholders across the country in face-to-face workshops, roundtables and bilaterals. The Home Affairs Department received 215 written submissions in response to a call for views; 156 of these are submissions are now available on the department's website. The minister for home affairs also established an Industry Advisory Panel to provide strategic advice to support the development of 2020 strategy. The consultation increased the Australian government's understanding on how every part of government, business, and the community can help to implement the Cyber Security Strategy 2020

Consultation on the EU Joint Cyber Unit

On June 23, 2021 the European Commission laid out a vision to build a new Joint Cyber Unit to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union. The Joint Cyber Unit's proposed aims are to bring together resources and expertise available to the EU and its member states, creating an effective virtual and physical platform of cooperation. The proposal hopes to have the unit operational and fully established by June 30, 2022.

As the Joint Cyber Unit is being shaped there is an opportunity for the EU to initiate a transparent and inclusive process—and to include the views and expertise of all interdisciplinary stakeholders involved—whether public, private, or civil. Consultations, roundtables, or calls for papers may generate new ideas, identify ways of cooperation, or expose voids and pressing needs.

With the EU Joint Cyber Unit aiming to contribute to a safe digital economy and society, a logical step would be to give those same economic and societal actors a bottom-up line of communication with the EU.

Part Two

Implementing the EU Cybersecurity Strategy: Four Work Streams Recommended by the Agora Community

Part 2:

Implementing the EU Cybersecurity Strategy: Four Work Streams Recommended by the Agora Community

EU cyber policy is a concept increasingly evolving from a member-state-centric approach to EU-centric coordination. The next step is to add a multistakeholder dimension. In theory each stakeholder has its distinct role to play. The state is the security provider and acts through law and justice. The private sector contributes in its capacity as product innovator, first-line crisis responder, intelligence actor, and driver of Internet governance, as in the case of the Internet Protocol.[3] Civil communities compile, reflect, and communicate on the views of society. They also analyze public policies, identify potential gaps, and hold entities accountable for their actions. In reality this division of tasks is far more complex and increasingly blurry, especially in cyberspace. Hence the importance of creating an environment that brings all stakeholders together in a setting of equality and trust.

1 – Enhance Cross-Sectorial Lines of Communication

Strengthen the linkages between European cyber policy and non-governmental sectors. Create cyber capacity building projects that familiarize scientists or researchers with policy planning, and host workshops or meetings to facilitate a discourse on how to match their analysis with policy engineering and policy solutions.

To operationalize multistakeholderism the very first steps to take are building better communication between sectors, gaining better overview of what each stakeholder can contribute, and improving coordination in cyber capacity building.

Establishing good communication practices is critical. Too often policymakers, business executives, or academia lack direct lines of contact, or when they do communicate they do not understand each other's jargon.

3 The Internet Protocol (IP) is a set of requirements for addressing and routing data on the Internet.

Bad or ad hoc communication undermines mutual trust, effective information sharing, and cross-sectorial policy input. To change this, it is important to understand the motivations and benefits for all parties. This is especially true for researchers and public officials, two communities often the most distant from one another. Academia or scientists desire in general independence and information access. Policymakers desire in general expertise that is relevant, recommendations that are realistic, and research output that is in synch with political timelines. Capacity-building projects can help to bridge this gap and to create trust between communities. Training, guidelines, or protocols that steer toward frequent, structural, transparent contacts and dialogue between stakeholders can only lead to better understanding of the mutual dependencies, work practices, and benefits.

There is an opportunity to implement new EU initiatives, such as the Cyber Capacity Building Board, as the Cybersecurity Strategy calls for, in this spirit. This body would encompass relevant EU institutional stakeholders, and it would monitor progress and identify synergies and potential gaps in cyber capacity-building (CCB) efforts. As this new entity is being shaped, it could foresee a mechanism for systematic and comprehensive engagement with all stakeholders in EU CCB projects, from multisector practitioners involved in the implementation of cyber capacity-building actions to external experts in evaluating capacity development results. Thinking in these terms also means the board could extent regular invitations to local authorities, small and medium-sized enterprises, or NGOs involved in EU CCB projects to provide briefings on their direct experiences in the field.

Better communication is likely to lead to better understanding and overview of what nonstate cyber actors can contribute, in which areas, and to which goals. This is especially needed today for smaller-scale initiatives that often remain under the radar. Similarly, non-state actors do not always possess full understanding of who is who in governmental and EU structures. Existing research initiatives, networks, and dialogues could help coordinate efforts to build a better overview of EU-based cyber actors and link them to the desired policy actions of the Cybersecurity Strategy. This effort could come in the shape of an open-source website coordinated by a multistakeholder initiative that agrees to serve as the network point of contact. Such a platform would be particularly interesting to activate smaller cyber actors such as individuals or small and medium-sized enterprises, but also to identify social and economic actors who possess relevant expertise but do not yet choose to take part in cyber actions.

2 – Support Civil Society's Engagement and Improve its Preparedness

> **Link cyber policy goals to operational civil society platforms that strengthen bottom-up responses to cyberattacks. Create a coordinated regular review of the digital society that measures the resilience of critical infrastructure, but also assesses the preparedness of societies and citizens.**

The EU's critical infrastructure and essential services are increasingly interdependent and digitized. Ensuring resilience and stronger industrial and technological capacities in cybersecurity should mobilize all necessary regulatory, investment, and policy instruments. Adding a complementary civil society angle can bring several other benefits.

A recent European Commission proposal for an upgraded critical infrastructure directive focuses primarily on risk assessment, technical measures, and incident reporting. This directive is a much-needed top-down instrument to strengthen the resilience of critical infrastructure, but it does not include the important role of societal and cultural factors. Protecting critical infrastructure also requires: better awareness and cyber hygiene from employees, a culture of investments in capabilities (as regulations alone are often not enough), more openness from the critical infrastructure sectors in sharing nontechnical information regarding their preparedness and capabilities, and more trust and exchanges between critical-infrastructure executives and other actors such as industries or academia.

Effective bottom-up projects that help respond to cyberattacks are readily available in the nonstate community. But today their input on policy is limited because they are not well connected to protocols and frameworks that help feed responses into policymaking.

In this light, critical-infrastructure executives and employees could be involved in EU, private-sector, or civil exercises and simulations that outline what might happen during and after a cyberattack. Platforms like the European Cyber Agora can be useful to connect different communities, and to discuss with first-line responders, such as hospital doctors, bankers, or supply-chain engineers, how they view cyber threats and how they plan to address them. It must include third-party actors, such as smaller supply or logistical contractors of larger infrastructures. Nonstate initiatives such as the Cybersecurity Tech Accord[1] have in this regard a wealth of expertise to share with policymakers. Here cooperation with the newly established European Digital Innovation Hub on webinars, simulations, and other public activities would make sense. Engaging with ethical hackers who infiltrate networks and expose vulnerabilities may still be controversial, but it presents an opportunity to gather lessons learned and best practices. Taken together, these steps can help to build awareness for the cyber resilience of infrastructure, but also of people and societies.

4 More information: https://cybertechaccord.org/

3 – Increase Operational Capacity to Prevent, Deter, and Respond

Improve the efficiency of the EU Cyber Diplomacy Toolbox by strengthening preventive cybersecurity initiatives. Facilitate the release of empirical data for multistakeholder initiatives that proactively index or identify enablers of malicious cyber activities.

Cyber incidents can cause enormous damage. EU institutions, bodies, and agencies as well as member-state authorities, are responsible for preventing, deterring, and responding to cyber threats. Nonstate actors can play a part in this regard but their inclusion in these processes is still limited.

The EU has made great progress in cataloging its cyber capabilities and in identifying technical gaps. But a greater hurdle in achieving cyber peace is the fact that it cannot map malicious activity of state and nonstate actors in cyberspace in a way that is satisfactory. There is also no mechanism or measurement to track commitments to responsible behavior or adherence to international principles. Multistakeholder initiatives to address this gap are under way, mainly through the Paris Call Working Group 5 (Building a Global Stability Index of Cyberspace). The benefit of such an index would be to understand roles and responsibilities of different actors in cyberspace, to identify and map commitments and adherence to cyber norms, and to understand how malicious activities have a concrete impact on human security, dignity, and equity. There is a lot the EU can do to actively support stakeholders in this initiative, from facilitating access to data to allocating resources so the index can be regularly updated and remain relevant in time.

This matters because such a multistakeholder-driven index can help to increase the EU's and all other cyber actors' situational awareness. As geopolitical tensions complicate our ability to address the causes of cyber threats it also makes it harder to understand the factors and circumstances that make cyber operations more likely and more successful. In this sense, the EU Cybersecurity Strategy says little about the enablers of cyber conflict and how to

tackle them. Here it matters not only to look at variable factors, like diplomatic reciprocity or geopolitical developments, but also to find the constant governance, societal, and technical enablers that make cyberattacks more successful. For instance, the degree of acceptance for a ransomware culture, or deliberate government policies that enable malicious cyber proxies.

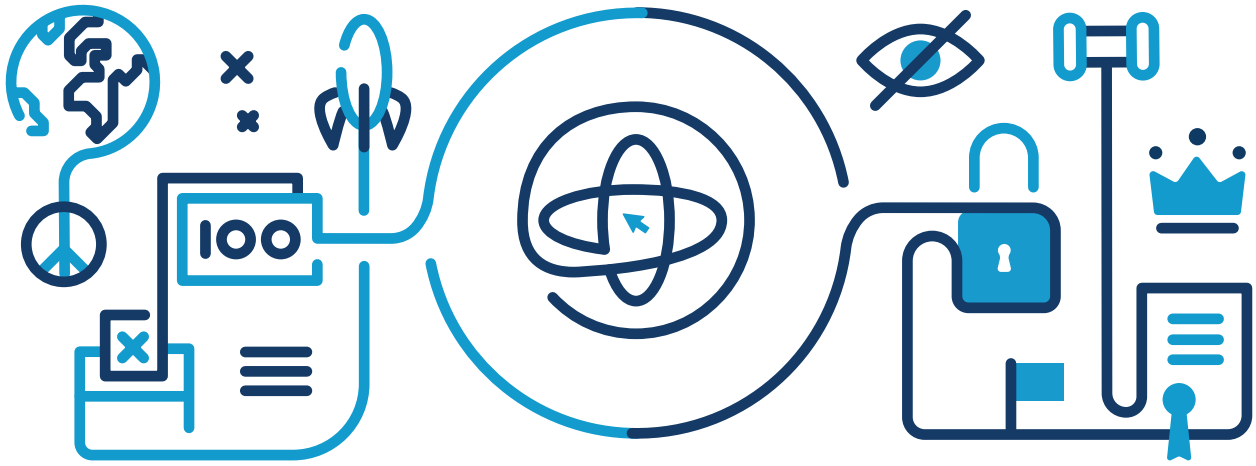
The challenge for the EU is to better understand these interconnected realities, to create an inclusive overview of strategic enablers, and to work with different sectors to mitigate their impact. Calculating or identifying potential aggressors is important in attributing attacks, which would activate the EU Cyber Diplomacy Toolbox, a range of restrictive measures the EU can impose on malicious cyber actors. But public attribution is a highly complex process involving many considerations and stakeholders. The toolbox needs to be informed not only by technical forensics, but also by geopolitical strategy, multistakeholder intelligence, and coordinated pragmatism. Any member of the security community can be responsible for cyber incidents—from an individual to a civil or commercial activity group, to a government. Therefore, attribution will also benefit from community responses. Such mindset is increasingly emerging, but there is still space for improvement. Implementing a fact-based and data-driven cyber policy to effectively prevent, deter, and respond is only possible if all stakeholders are working together.

4 – Advance a Global and Open Cyberspace

> **Resolve the conundrum between EU commitments to open cyberspace and calls for strategic autonomy and technological sovereignty. Develop a credible narrative to convince third countries of the benefits of a democratic cyberspace, and the threat of a splintered Internet.**

The EU should work with international partners to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms, and democratic values that promote social, economic, and political development globally, and build a security union

The EU Cybersecurity Strategy should also be a geopolitical tool, aimed at sustaining Europe's technological sovereignty and strategic autonomy. New technologies and cyberspace have an enormous impact on political, economic, and military capabilities. Much of today's great-power competition is already centered on the quest for technological leadership and the control over supply chains in information and communications technologies.
This also raises questions around digital authoritarianism and the protection of open and democratic cyberspace. China and Russia, in particular, are champions of a splintered Internet vision, while the EU is only starting to think at earnest about its own narrative. The challenge for the EU will be to balance its commitments to a democratic, open, stable, peaceful, and secure cyberspace and its desire to achieve digital sovereignty and strategic autonomy. Calls for sovereignty or autonomy in cyberspace might be exploited by those seeking a fragmentation of the Internet, or creating a "splinternet". Platforms like the CyberSec Forum, EU Cyber Direct, or the European Cyber Agora may serve as a helpful tool to collect diverse views on this conundrum and to develop a credible narrative marrying both concepts. Solving this equation matters if the EU is to convince third countries, or to position itself in global processes such as the UN or the Paris Call, and to secure its leadership in cyberspace in general.



Resilience against authoritarianism is essential because in the digital age fundamental freedoms and human rights are under stress in areas such as freedom of association, censorship, and surveillance. With approximately 5 billion Internet users and 4 billion social media users worldwide, the stakes are high. The EU is determined to tackle these challenges through data protection and privacy, combating Internet shutdowns, fighting against cybercrime and disinformation, and a human-rights-based approach on new technologies (for instance, ethical standards around artificial intelligence). But to become a human-rights champion in cyberspace, it will need to develop an inclusive democratic narrative. Such narrative will also be beneficial to operationalize the EU Action Plan on Human Rights and Democracy 2020–2024.

In its quest for allies, the EU will likely find them among global democracies. It should also look across the Atlantic. The United States and Canada agree broadly on the normative, economic, and geopolitical necessity of stability in cyberspace. The Biden administration is committed to addressing cross-cutting issues in cyberspace through multilateral and multistakeholder engagement. It is also seeking to revitalize the relationship with the EU and raise transatlantic ambitions with respect to values such as democracy, human rights, or economic opportunity. The United States has consequently welcomed EU policies such as the new Cybersecurity Strategy or the 5G Toolbox. Coordinated actions with transatlantic or global partners has distinctive potential to generate advantage for the EU without jeopardizing its strategic autonomy or technological sovereignty.

Conclusion

Cybersecurity inspires continuous adaptation. The time for a new adaptation is now—one that brings all actors together to develop inclusive solutions for European cybersecurity. Yet, the EU institutions and member states could still improve their engagement with stakeholders. The political discourse over the years has made great strides forward and has resulted in the creation of several dialogue platforms. But governmental actions to operationalize multistakeholder input remains in many cases ad hoc. Nevertheless, the ingredients for regular and systematic cross-sectorial cyber cooperation are already available, but they need to be better coordinated. To bring them together a different mindset is needed. There is increasing political, economic, societal, and academic motivation to think in this direction.

The EU Cybersecurity Strategy must serve as a bedrock to coordinate future actions in this spirit. New initiatives, like the proposed EU Joint Cyber Unit, will be more effective if they are created in consultation with diverse communities. Inclusivity also spurs legitimacy. The EU has an opportunity to export this mindset to international fora that have a stake in cybersecurity. There is a number of newly announced platforms to look out for, such as the EU-U.S. Trade & Technology Council, the NATO Defence Innovation Accelerator or the UN Programme of Action.
Finally, multistakeholderism alone will not do the trick. The EU's cyber power must be underpinned by global alliances. In many cases, Canada and the United States will be its like-minded partners, but other countries too share its interest in a safe and responsible cyberspace. Global alliances are set to define the EU's normative power on cybersecurity.

The European Cyber Agora 2021 is facilitated by

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

Microsoft

EU CYBER DIRECT