Non-Paper on EU Cyber Diplomacy
by Estonia, France, Germany, Poland, Portugal and Slovenia

The Context: Changing Circumstances

Since the adoption of the Council Conclusions on Cyber Diplomacy in February 2015, several interlinked developments in the political, economic, societal and technological spheres have increased the importance of cyberspace and highlight the need for a renewed strategic reference document at EU level for cyber diplomacy:

Due to the inexorable progress of digitalisation in almost all areas of life, including in the global economy and the private lives of citizens, the need to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with regard to the processing of personal data, and the need to protect critical infrastructure in the EU and its Member States against malicious cyber-attacks are of ever-increasing importance.

Cyberspace is continuously generating novel attack targets and vectors and cyber-attacks are growing in terms of scope, frequency and sophistication as well as the damage they inflict, and state and non-state actors, including proxies, are increasingly willing to pursue their objectives by conducting malicious cyber activities varying in scope, scale, duration, intensity, complexity, sophistication and impact.

Malicious cyber activities can serve several purposes and take various forms, including attacks against infrastructure, cyber-espionage, intellectual property theft, cybercrime, and possibly also attacks in the context of hybrid threats.

The COVID-19 pandemic has demonstrated the increasing dependence on fast and stable connectivity and that a functioning, stable and secure cyberspace is an important condition for this.

Cyberspace has increasingly become an area of strategic competition between states which reflects the dynamic geopolitical environment in recent years, and technological innovations have increasingly become points of contention between states due to their growing significance for economic and military competitiveness, which has also resulted in a technological confrontation between major actors.

More confrontational approaches in the technological realm may lead to certain decoupling effects and to a further severing of global supply chains and cooperation with regard to research and innovation, including in the area of cyber security, as well as to a potential fracturing of the global internet, which is noted with concern.

The EU and its Member States have to clearly define their role in the context of growing competition between major actors that are increasingly willing to shape the digital environment and the discussion surrounding it, meaning that the EU and its Member States have to assert themselves in international cyberspace norm-setting and technological standard-setting bodies.

States with an authoritarian outlook are increasingly trying to enforce their interests in cyberspace and in the technological realm and the EU and its Member States have to react by promoting their values and interests, which include human rights, prosperity, security and Europe´s digital sovereignty.

Non-Paper on EU Cyber Diplomacy
by Estonia, France, Germany, Poland, Portugal and Slovenia

The use and deployment of technologies to track, surveil, anticipate or even grade the behaviour of citizens in a repressive and unprecedented way, and the use of digital tools by authoritarian states that is contrary to the idea of a free, open and global internet and international human rights law as well as plans by some countries to build an alternative internet regulated by the State are noted with concern.

Protection of its Citizens and Modern Societies

Recent EU cyber-related initiatives aimed at protecting its citizens and the resilience of its modern societies and the related data and critical infrastructure against malicious activities in cyberspace, such as the renewed Cyber Security Strategy, Review of the NIS Directive and the EU 5G Toolbox with its objective of establishing a coordinated European approach aimed at mitigating the main cyber security risks of 5G networks, are welcomed and the importance of maintaining and strengthening coherence among the EU cyber and digital initiatives is noted.

With the advent of innovative technologies such as artificial intelligence, the Internet of Things or 5G, new possible targets and vectors are emerging in cyberspace, which also have to be reflected in global debates concerning norms of behaviour in cyberspace. Furthermore, cybercrime actors are steadily developing new forms of malicious activities to exploit vulnerabilities in cyberspace.

While digital technologies and increased connectivity are key components of modern societies and bring major benefits in terms of growth and prosperity, at the same time citizens, companies and governments are, especially in the context of the COVID-19 pandemic, more and more exposed to offenses in the field of cybercrime, which are steadily increasing in number and sophistication. Thus, the EU and its Member States reiterate the need for a coordinated and determined fight against cybercrime and continue to promote the Council of Europe Convention on Cybercrime, also known as the Budapest Convention, and the negotiations on the Second Additional Protocol to the Budapest Convention, as an important framework for international cooperation in the fight against cybercrime.

Regarding access to digital evidence, the EU and its Member States first recognize encryption as an important tool for the protection of cybersecurity and fundamental rights, such as privacy, including the confidentiality of communications, and personal data. The EU and its Member States are invited to find solutions that allow law enforcement and other competent authorities to gain lawful access to digital evidence concerning malicious cyber activities, without prohibiting or generally weakening encryption, and in full respect of privacy and fair trial guarantees consistent with applicable law.

The EU and its Member States acknowledge in that context the work done by EUROPOL and similar European and international institutions with a view to supporting and coordinating investigations of cyber-attacks and cybercrime among the Member States.

The EU, for instance in the context of the Horizon Europe framework programme, and its Member States are encouraged to further invest in cyber security research, including in the areas of digital forensics analysis, threat intelligence and incident response in the face of malicious activities in cyberspace.

Non-Paper on EU Cyber Diplomacy
by Estonia, France, Germany, Poland, Portugal and Slovenia

Promotion and Protection of Human Rights in Cyberspace

It is of central importance for the EU and its Member States to uphold and strengthen individuals' human rights and fundamental freedoms equally online and offline.

The steady increase and spread of the use and export of technologies that could be and are already employed for mass surveillance, censorship or other measures violating or abusing individuals' human rights and fundamental freedoms and the related unprecedented possibilities of societal control can increase the attractiveness of a digitalised authoritarian model of governance and the use of technologies for unlawful and oppressive purposes runs contrary to the values and interests of the EU and its Member States. Thus, the EU and its Member States should continue to promote and implement the idea of developing and employing digital technologies in a democratic way that benefits both the social well-being of its citizens and prosperity, with full respect for the rule of law and human rights.

The worrying trend towards increasing internet censorship, which can violate human rights and in particular impedes freedom of expression, free and equal access to information and the right to assembly and association and puts restrictions on human rights defenders in authoritarian states, is noted with concern and the EU and its Member States underline their commitment to a global internet as an open, neutral, single, free and non-fragmented framework.

The EU and its Member States are called upon:

- to promote and protect human rights and fundamental freedoms in cyberspace, including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy, as well as the protection against mass surveillance, and in particular to support persons in vulnerable situations or marginalised groups such as ethnic, religious and political minorities and dissidents against oppression via digital technologies globally, and to protect civil society space also online;

- to promote and protect international human rights in cyberspace by working towards human-rights-friendly regulatory frameworks;

- to encourage the sharing of good practices on the promotion and protection of fundamental rights in cyberspace with all relevant stakeholders, and to do the same concerning the use and export of technologies that could be misused for surveillance or censorship purposes and in general concerning dual-use technologies;

- to promote universal, affordable and equal access to the internet and in particular the empowerment of women and girls and persons in vulnerable situations or marginalised groups in policy development and regarding use of the internet and

- to steadily assess whether novel digital technologies and their application are beneficial for democracy and human rights and whether they can be exploited for malicious activities.

Non-Paper on EU Cyber Diplomacy
by Estonia, France, Germany, Poland, Portugal and Slovenia

Cyberspace as an Enabler for Economic Prosperity and Social Well-Being

The EU and its Member States acknowledge the pervasive impact that digitalisation has on political, social and economic development, along with the fact that access to and use of a free and secure cyberspace is of prime importance for economic growth and innovation as well as for the social well-being of free and modern societies.

The importance of cyber security for innovative applications and technologies, including artificial intelligence or the Internet of Things as well as for Common European data spaces, as is stated in the EU's data strategy, which will ensure the Union's global competitiveness and data sovereignty while keeping companies and individuals who generate the data in control, is acknowledged.

Europe's digital economy and society are closely interlinked with international developments and the EU and its Member States are reliant on close political, economic and social interactions on a global level, which creates opportunities, such as growth and prosperity effects, for its remarkable industrial base and vibrant digital market, but at the same time entails challenges, including the management of external dependencies in the technological realm and malicious cyber activities against critical infrastructure, electronic communications networks and services outside of the Union.

Cyberspace as a Key Area for the EU's Foreign Policy and Digital Sovereignty

Due to the increasing importance of cyberspace for several areas of life and the growing significance of digital technologies for power projection on the international stage, cyber diplomacy should be considered an important tool for fulfilling the objectives and interests of the EU.

The protection and reinforcement of Europe's digital sovereignty in the EU stands in direct connection with cyber security, as it ensures trust in digital technologies and the digital transformation process. Thus, a coherent international cyberspace policy must be considered a key component of the determined engagement of the EU and its Member States with a view to reinforcing their digital sovereignty by having the ability and the will to shape global debates, which reflects the EU's values as well as its strategic and economic interests, and the capacity to act self-assertively in cyberspace, which should not be confused with isolating itself or striving for digital or technological autarky.

Through its engagement – within the EU and beyond – with regard to setting norms of behaviour and establishing regulations concerning cyberspace and its self-conception as a preventive actor in contributing to a secure, stable and open cyberspace, the EU serves as an international point of reference, especially for states which want to avoid confrontational approaches internationally and adhere to international law in cyberspace, and the EU positions itself as a champion of and force for peaceful relations, conflict prevention and greater stability in cyberspace.

The EU with its human-centred approach is in an excellent position to set sophisticated cyber-related and technology standards, such as the General Data Protection Regulation (GDPR) or the ethical and legal framework proposed by the AI White Paper concerning high-risk applications, which serves as a model for other regions.

Such a coherent international cyberspace policy of the EU – especially in the context of the previously mentioned numerous and interlinked developments in the political, economic, societal and technological spheres – should serve:

- the EU's foreign and security policy objectives and broader values, as stated in the EU Global Strategy, with cyber diplomacy being an integral part of the pursuit of these goals in the context of the Common Foreign and Security Policy (CFSP), and with activities in cyberspace being conceived jointly and in line with contextual developments at international level;
- the purpose of protection of its citizens and modern societies, and of the related data and critical infrastructures, against malicious activities in cyberspace, as well as the integrity and security of the EU and
- the purpose of promotion and protection of the fundamental EU values of democracy, human rights, gender and digital equality and the rule of law in cyberspace, including the right of expression and equal access to and secure use of information and communication technology (ICT) and the internet, on the global stage, especially in light of the increasing misuse of new technologies that leads to human rights and privacy violations.

In order to achieve the previously mentioned goals, the EU possesses a broad portfolio of cyber diplomacy instruments, which should be seen as cohesive and mutually complementary, in particular:

- determined engagement in norm-setting processes in international organisations such as the UN to support norms of state behaviour in cyberspace, including through supporting the establishment of a Programme of Action (PoA) for Advancing responsible States behaviour in cyberspace, as constructive outcome of both the current UN GGE and OEWG processes, addressing the need for inclusivity;
- determined engagement in setting cyber-related and technical standards and regulations on a global level and the development of a cohesive approach and the assumption of an active role in ICT standard setting in the context of public private partnerships (PPP), especially in light of the increased activity in this area by emerging powers and the importance of technical standards for business development as well as for safety and reliability;
- possible application of its Cyber Diplomacy Toolbox in case of malicious cyber activities against the EU, its Member States and third states, by using a number of adequate and determined measures at its disposal which are organised into the five categories of preventive measures, cooperative measures, stability measures, EU support to Member States' lawful responses, and restrictive measures and that strengthen Europe's capacity to act in cyberspace;
- capacity building measures in third countries that actively contribute to the promotion and protection of the right to freedom of expression and to universal and equal access to information and that enable citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructure; in that context, the EU and its Member States can resort to best practices such as the NIS Directive and further internal initiatives and regulations;
- structured and overarching cyber dialogues and consultations with third states and with other international organisations and regional bodies in order to increase security and reliability in cyberspace;
- confidence-building measures to build trust and dependable relationships between states and international actors in cyberspace and

- multi-stakeholder engagement with several actors, including the public and private sector, as well as with civil society and academia, to deal with this multi-sector and multi-disciplinary field.

Since the Council Conclusions on Cyber Diplomacy of February 2015, many of the mentioned instruments have undergone development and have thereby become considerably more sophisticated, but at the same time the EU and its Member States are called upon to further develop these instruments in terms of their effectiveness and sophistication and to continue to develop a stronger, more cohesive approach.

Strategic Engagement with Key Partners and International Organisations

Many recent cyberspace developments have taken place in different international organisations, including the UN, the Council of Europe, OSCE, OECD, NATO, AU, OAS, ASEAN, ARF, and the EU and its Member States are invited to further engage in and with, as well as cooperate and coordinate with, these international and regional organisations.

Structured and overarching EU cyber dialogues and consultations have been conducted with countries such as Brazil, Canada, China, India, Japan, South Korea and the United States, and the EU will launch new ones, for instance with Ukraine. These dialogues may aim at building trust and reinforcing existing relationships, while also serving to exchange best practices concerning cyber security and to promote human rights and the rule of law, and will be further continued.

The significant progress achieved on EU-NATO cooperation in the field of cyber security and defence since the signature of the 2016 Warsaw and 2018 Brussels Joint Declarations and the importance of the full implementation of the common set of proposals are welcomed, the ongoing EU-NATO staff-to-staff dialogues on cyber defence, and cyber defence information sharing between the NCRIC and CERT-EU are appreciated, and further EU-NATO cooperation in cyber security and cyber, especially in the areas of training, education, cyber defence and technology innovation, and reciprocal participation in exercises is encouraged.

The implementation of the Cyber Security Confidence Building Measures in the OSCE, including both sets from 2013 and 2016, which are an important contribution to creating trust and dependable relationships among state actors and international organisations, are welcomed and should continue to be promoted.

Application of Existing International Law and Norms of State Behaviour

The EU and its Member States welcome the work done within the UN GGE, notably its 2010, 2013 and 2015 reports, with the publication of 11 voluntary norms of responsible state behaviour in cyberspace, and the consensus achieved that international law, in particular the Charter of the United Nations, is applicable to cyberspace and is essential to reduce risks and maintain peace and stability; the EU and its Member States also welcome the work done within the UN OEWG with its open, multi-stakeholder approach and the objective of further developing rules and norms of responsible behaviour in cyberspace and their implementation.

Non-Paper on EU Cyber Diplomacy
by Estonia, France, Germany, Poland, Portugal and Slovenia

Many aspects of the 2015 GGE report have been included in and implemented by EU strategies and frameworks, such as in the context of the NIS Directive or the Cyber Diplomacy Toolbox.

The EU and its Member States see recent developments, including complexity in the development and implementation of voluntary norms in the UN context in recent years as a basis and an incentive to further support and strengthen the international discussion on norms in cyberspace and to reinforce the EU's stance on the applicability of international law, and the EU and its Member States will further actively contribute to consolidating voluntary norms of behaviour on the international stage.

The work done by other regional organisations such as by the third ASEAN Ministerial Conference in 2018 or the norms adopted by the G-7 summit in 2017, which are based on the GGE 2015 norms, is welcomed.

Ongoing efforts to improve mechanisms for global digital cooperation, in particular those under the auspices of the UN Secretary-General, including his Roadmap for Digital Cooperation as well as the Options Paper for the Future of Global Digital Cooperation, and to build on existing structures, ensure inclusive and multi-stakeholder processes and create stronger links between internet governance fora, are welcomed.

The important part that the EU and its Member States played in international cyberspace policy and internet governance debates and events, such as the Paris Call for Trust and Security in Cyberspace and the Global Commission for Stability in Cyberspace, and other similar initiatives, is emphasized.

While initiatives from state actors, the private sector and civil society aiming at developing rules, norms and principles are strongly welcomed, a potential growing fragmentation of cyber norms may require stronger coordination efforts among the EU and its Member States as well as with its global partners, and the EU and its Member States are invited to engage accordingly.

EU Cyber Diplomacy Toolbox

The added value of the Cyber Diplomacy Toolbox, introduced by the Conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, which in a transparent and resolute way provides the EU and its Member States with instruments to give adequate and determined responses to malicious cyber activities with a wide range of diplomatic, political and economic measures, is strongly welcomed. The Toolbox comprises:

(i) Preventive Measures,
(ii) Cooperative Measures,
(iii) Stability Measures,
(iv) Restrictive Measures and
(v) Possible EU support to Member States' lawful responses.

The EU is steadily and fully committed to promoting the benefits of adhering to norms of responsible state behaviour in cyberspace, and will not shy away from imposing costs on malicious actors violating those norms, and the application of the Toolbox and in particular restrictive measures aim to change the behaviour of state and non-state actors and increase the incentive to adhere to and

implement the respective norms, as well as to serve as an instrument of working towards a culture of compliance and responsibility in cyberspace.

The EU has recently invoked the Cyber Diplomacy Toolbox and applied restrictive measures in response to malicious cyber activities and is strongly committed to continuing to do so in the event of further norm-violating activities in a manner proportionate to the scope, duration, intensity, complexity, sophistication and impact of the activities in question.

These instruments should be seen in the context of a broad cyber diplomacy portfolio that the EU and its Member States have at their disposal, alongside other instruments; they are designed to have an impact on the cost-benefit calculations of actors conducting malicious activities in cyberspace.

The EU and its Member States are invited to place emphasis on the further development and sophistication of the decision-making and invocation processes of the Cyber Diplomacy Toolbox by drawing lessons from its initial applications.

Cyber Capacity Building and Development

The Council Conclusions on EU External Cyber Capacity Building Guidelines, in which the need to prioritise the EU's cyber capacity building efforts in its neighbourhood is stressed, are recalled and the importance of cyber capacity building in partner countries and regions as a strategic building block of the continuing cyber diplomacy efforts of the EU for the sake of promoting and protecting human rights, the rule of law, gender digital equality, security, inclusive growth and sustainable development, as well as strengthening the resilience of network systems and digital infrastructure along the lines that all developed and most developing countries depend on each other in the ever more globally networked world, is emphasised.

The importance of access to, and unhindered, uncensored and non-discriminatory use of, open and secure information and communication technology (ICT) for fostering open societies and enabling economic growth and social development globally, is stated.

The importance of promoting the EU’s political, economic and strategic interests in the face of expanding and complex international discussions on cyber issues, and of ensuring that the international cyber capacity building and cooperation efforts led by the EU and its Member States follow overarching guidance to ensure a coherent, holistic and effective approach, is emphasised.

The EU and its Member States – including through several capacity building projects on cyber diplomacy, cyber security, cyber resilience and cybercrime – are at the forefront in the design and implementation of cyber capacity building efforts in light of the growing demand for cyber capacity building on the global stage and are providing substantial assistance in the areas of human resources and knowledge development, as well as institutional and organisational reforms and adaptions.

Increasing initiatives and stakeholders in the sphere of cyber capacity building internationally creates opportunities for synergies and burden-sharing but also poses challenges with regard to duplication and thus increasing EU-wide coordination efforts in this regard are welcomed.

Non-Paper on EU Cyber Diplomacy
by Estonia, France, Germany, Poland, Portugal and Slovenia

Summary - Key Principles

The EU and its Member States are fully committed to a global, open, free, stable and secure cyberspace, which is of ever-increasing importance for the continued prosperity, growth, security, well-being, connectivity and integrity of our free and democratic societies.

The EU and its Member States are committed to ensuring that cyberspace fully reflects and respects the core EU values of the rule of law, human rights and fundamental freedoms, gender and digital equality, as well as inclusive growth and sustainable development, and that the internet should remain a forum for free expression within the bounds of the law.

The EU's cyber diplomacy is an important part of the Union's efforts to protect and reinforce its digital sovereignty and cyberspace is central for economic prosperity, development and security, where norms for responsible state behaviour, international law and the rule of law should be upheld, and cyber diplomacy instruments are important for seizing opportunities and addressing challenges in these areas.

Existing international law, including the UN Charter, international humanitarian law and human rights law, as well as the rule of law and norms of behaviour, apply in cyberspace, and the EU is fully committed to further working with its global partners to implement these norms internationally.

The EU and its Member States emphasise the importance of processes for the elaboration of responsible state behaviour in cyberspace under way in international organisations such as in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications (UN GGE) and in the UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (UN OEWG), as well as the ability of the EU and its Member States to shape the global debates on the future of cyberspace, and additional and complementary initiatives and frameworks regarding norms of responsible state behaviour, confidence building measures and capacity building with relation to cyberspace are welcomed. In that regard, the EU and its Member States support the proposal to establish a Programme of Action (PoA) for advancing responsible state behaviour in cyberspace. This proposal could be a constructive outcome of both the current UN GGE and OEWG processes, addressing the need for inclusivity.

The significance of cyber diplomacy instruments at EU level, notably the Cyber Diplomacy Toolbox introduced in 2017, is underlined; the Toolbox in a transparent and resolute way provides the EU and its Member States with instruments to prevent, discourage, deter and give adequate and determined responses to malicious activities in cyberspace.

The EU and its Member States are committed to the importance of all stakeholders' involvement in global norm-setting processes and governance of the internet; these explicitly include academia, civil society and the private sector.

An international cyberspace policy of the EU must be considered an important part of the EU's foreign and security policy objectives and broader values, and such a policy should complement existing policies in the areas of the Internal Market and Justice and Home Affairs, in particular the European Commission's recent Communication on "Shaping Europe's digital future" and "A European strategy for data", as well as the White Paper "On Artificial Intelligence – A European approach to excellence and trust".